IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 19, 2018, accepted January 17, 2019, date of publication February 6, 2019, date of current version April 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2897923

A Markov Multi-Phase Transferable Belief Model for Cyber Situational Awareness

GEORGIOS IOANNOU[1], PANOS LOUVIERIS[1], AND NATALIE CLEWLEY[2]
[1]Department of Computer Science, Brunel University London, Uxbridge UB8 3PH, U.K.
[2]Centre for Electronic Warfare, Information and Cyber, Defence Academy, Cranfield University, Shrivenham SN6 8LA, U.K.

Corresponding author: Panos Louvieris (panos.louvieris@brunel.ac.uk)

This work was supported in part by the UK Defence Science and Technology Laboratory, under Grant DSTLX1000048609.

ABSTRACT eXfiltration Advanced Persistent Threats (XAPTs) increasingly account for incidents concerned with critical information exfiltration from High Valued Targets (HVTs). Existing Cyber Defence frameworks and data fusion models cannot cope with XAPTs due to a lack of provision for multi-phase attacks characterized by uncertainty and conflicting information. The Markov Multi-phase Transferable Belief Model (MM-TBM) extends the Transferable Belief Model to address the multi-phase nature of cyber-attacks and to obtain previously indeterminable Cyber SA. As a data fusion technique, MM-TBM constitutes a novel approach for performing hypothesis assessment and evidence combination across phases, by means of a new combination rule, called the Multi-phase Combination Rule with conflict Reset (MCR^2). The impact of MM-TBM as a Cyber Situational Awareness capability and its implications as a multi-phase data fusion theory have been empirically validated through a series of scenario-based Cyber SA experiments for detecting, tracking, and predicting XAPTs.

INDEX TERMS APT, combination rule, conflict, cyberspace, kill-chain, Markov processes, prediction, sensor fusion, situational awareness, uncertainty.

I. INTRODUCTION

Cyber attacks account for an estimated $1 trillion annual cost [1], of which $445 billion is attributable to cyber-crime [2]. Some of the most prominent cyber incidents, such as the US Investigations Services hack [3], the Equifax hack [4], the Home Depot and the JP Morgan Chase incidents [5] involve massive information theft, i.e. internal communications and sensitive customer information. High-profile cyber incidents are the results of eXfiltration Advanced Persistent Threat (XAPT) campaigns [6]. XAPTs are launched by individuals, organizations or state-sponsored representatives that employ a wide range of sophisticated reconnaissance and information gathering tools. The motivations for these multi-phased attack vectors are systems sabotage, extortion or stealing proprietary information from high-valued assets and Critical Information Infrastructure [7].

Cyber network operators are required to retain concise and relevant Situational Awareness (SA), and often face the challenge of protecting critical information from XAPT attacks within a contested, congested, cluttered connected and constrained cyberspace [8]. A solution for informing SA against XAPTs is provided by the kill-chain [9]–[11] which models how an XAPT takes place as a sequence of distinct and finite attack phases. Each phase serves a certain purpose within the attacker's plan in order to reach their ultimate target behind defenses and exfiltrate information from a High Valued Target. The kill-chain model serves as a valid starting point for developing new theories and approaches where multi-phased attacks are concerned, taking into account the characteristics of the cyberspace, the limitations of intrusion detection systems and existing cyber threat models.

Cyber SA systems for facilitating decision support are tightly coupled with data fusion systems [12] which provide the means for combining the various information cues within the cyberspace for informing Levels 1 and 2 of SA [13]–[15]. Data fusion techniques are designed to handle a large number of sources of evidence which makes them suitable for Computer Network Defence (CND) applications. Existing mathematical theories such as the Dempster-Shafer theory [16], the Transferable Belief Model [17] and Bayesian fusion [18] are used as data fusion methods for enhancing

The associate editor coordinating the review of this manuscript and approving it for publication was Hongli Dong.

Cyber SA [19]–[21]. However, these conventional data fusion theories are constrained to applications that do not consider multiple, causally linked hypothesis spaces. A review of the relevant literature [33]–[35] shows that research on developing theories for detecting multi-phased attacks like XAPTs is limited and does not take into account conflicting information and uncertainty within the sources of evidence. Moreover, the majority of scientific data fusion research has been concerned with eliminating the conflict within sources of evidence, by means of redistributing the associated conflict mass [22], adaptively switching between combination rules when conflict mass becomes high [23], discounting of the contradicting evidence sources [24] or by treating it as a consequence of measurement error [25].

This paper proposes an extension to the Transferable Belief Model [17], the Markov Multi-phase Transferable Belief Model (MM-TBM), for enhancing the SA of cyber network operators against XAPTs. As a Cyber SA system, MM-TBM links the kill-chain model to the concept of Attack trees [56], [57] which are graph structures that depict the potential sequence of actions an attacker may take. MM-TBM offers first-time capabilities such as Tracking and Prediction of XAPTs, multiple and concurrent attack detection and diagnostic functionality for handling situations of missing evidence. In the field of data fusion, MM-TBM is the first approach which is oriented towards managing the multi-phase class of problems that satisfies the Markov property by means of the Multi-phase Combination Rule with Reset (MCR^2). This is the first combination rule that handles multiple causally-linked hypothesis spaces across the phases of a multi-phased cyber-attack by migrating within these spaces according to the attack's progression. Building on the concepts developed by [26], MM-TBM utilizes conflict as an indicator for identifying paradoxes in order to improve attack detection capability. Furthermore, based on the concept of Bayesian updating, a diagnostic formula for tree structures is proposed which allows for handling situations of hidden evidence.

II. RELATED WORK

A. XAPT DETECTION

Several proposals for detecting or preventing data exfiltration attacks exist, such as profiling legitimate user behavior and anomaly detection [27], [28], deep packet inspection techniques [29], stochastic forensics upon the filesystem [30] or a combination of traffic behavior analysis and file access patterns [31]. Dube *et al.* [32] consider XAPTs simply as attacks that contain sophisticated malware and focus on developing a solution that identifies malware based on the assets they may target.

Under a kill-chain perspective, these solutions operate exclusively at the final phase where attackers are close to achieving their mission objectives. Although these techniques may under certain circumstances be proven effective in identifying the evidence relevant to the data being exfiltrated from a protected computer network, they fail to adhere to the multi-phase nature of XAPTs. The data exfiltration phase, which is the adversary's main effort, occurs at the final stage of an XAPT which implies that single-phase approaches [27]–[32] do not pick up or utilize important cues and necessary evidence, thereby resulting in ''perception myopia''.

Preliminary work on the development of multi-phase based detection for Advanced Persistent Threats [33]–[35] is now considered. In [33] a scheme is proposed for correlating user behavior, network transactions and security policy authorizations, but does not consider the sequence that links the distinct attack phases. A graph-based framework [34] has been developed for modelling attack behavior, though user input is necessary for correlating alert related information. A 3D Attack tree representation of XAPTs is proposed in [35] but does not consider uncertainty and conflict. It is therefore apparent that the full range of XAPT characteristics are not sufficiently addressed, hence there is a gap within the state-of-the-art in Cyber Defence.

B. CYBER SITUATIONAL AWARENESS

Existing research [18] on Cyber SA commonly extends the concepts defined by Endsley [36] and the JDL data fusion model [37]. The proposed models rely on risk-assessment [39], [40], visualization of network traffic [41] or converting raw data from the network to an ontological structure for interpretation by users [42].

Markov models are commonly applied for Situational Awareness in Cyber Defence [67]–[69] and other applications such as maritime surveillance [70]. Shen *et al.* [67] use insights from game theory to improve situational awareness by fusing sensor data from the perspective of a Markov game-theoretic model to make predictions about future attack states. Situational Awareness for insider cyber threats is considered in [68] where Hidden Markov Models are used in conjunction with Dynamic Bayesian Networks for foreseeing future behavior of adversaries. Similarly, behavioral patterns are extracted from historical attacks in terms of attack sequence and transition probabilities in [69] to generate Variable Length Markov models. However, these models are not robust enough to handle missing evidence that correspond to attack steps; hence they cannot maintain tracking of an attack path when a phase is not detected.

Cyber defenders are facing a great deal of uncertainty [40] which could lead to distorted Cyber SA. Special reference is given to uncertainty management, with existing approaches being insufficient [43]. With respect to multi-phased cyber-attacks like XAPTs, Cyber SA research has focused primarily on attack model definitions such as kill-chains. Even though there exists a large body of research in this area, work has been limited to the single activity of attacks [45]. There is a lack of research on methods or tools that provide the capability for informing Cyber SA across all the phases of the attack kill-chain, i.e., in the presence of an XAPT. Consequently, Cyber SA is informed by evidence from individual phases of

an XAPT with no clear linking between these phases, forming an incomplete operational picture.

C. DATA FUSION AND THEORIES OF EVIDENCE

Cyber SA systems rely heavily on data fusion techniques to facilitate the combination of the various information cues within the cyberspace for informing Levels 1 and 2 of SA [13]–[15]. Decision support systems for enhancing Cyber SA are tightly coupled with data fusion systems [12].

Data fusion is the process of combining data collected from various sources within an environment in order to develop a concise and accurate representation of the environment's true state. Within operational environments that are characterized by uncertainty and conflict, evidence theories such as Dempster-Shafer and the Transferable Belief Model [16], [17], [49] are employed which utilize combination rules for fusing heterogeneous pieces of evidence and reasoning under uncertainty. The core component of Dempster-Shafer theory is Dempster's rule of combination. This rule is used to combine beliefs from more than one source (or agents). The rule is defined as:

$$m_{12}(A) = \frac{1}{1-k} \sum_{B \cap C} m_1(B) m_2(C)$$

where

$$k = \sum_{B \cap C = \varnothing} m_1(B) m_2(C), \quad k \neq 1$$

The term m_{12} represents the belief mass derived by combining the belief masses m_1 and m_2. The rule of combination is the 'fusion' part of Dempster-Shafer theory (DST). Dempster's rule can be used to combine the belief assignments that are reported from multiple sources of evidence, provided that they refer to the same power set 2^{Ω}. The denominator in Dempster's rule of combination is called the normalization factor. Through this normalization, the rule redistributes the calculated conflict (represented by k) evenly across the hypotheses.

D. THE MULTI-PHASE GAP IN DATA FUSION

The kill-chain model is a convenient expression for the phases of an XAPT. Each attack phase has certain pieces of evidence associated with it. These attack phases and their corresponding pieces of evidence can be pinpointed by conducting a security assessment of the computer network.

Moreover, each attack phase constitutes a single, isolated hypothesis space which is associated with a specific pool of evidence. Essentially, the number of 'ground-truths' is equal to the number of attack phases. If one attempts to approach this problem using DST or TBM, a single frame of discernment (FoD) would be used and it would have to include all the hypothesis sub-spaces that are concerned with each phase. Under the traditional approaches ([16], [17]), a complete attack path would comprise of several members of the frame of discernment. This is a violation of the mutual exclusivity property which renders DST and TBM impracticable for multi-phase problems.

An additional implication of conventional fusion techniques ([16], [17]) stems from the characteristics of the cyberspace. A computer network can be subject to multiple concurrent cyber-attacks (that may or may not be part of an XAPT) which generate a vast amount of cyber evidence. Only a subset of this evidence would be relevant to an XAPT. Under these conditions, it is vital to distinguish between the relevant and irrelevant pieces of evidence in order to track an XAPT efficiently. Using a conventional fusion technique would allow heterogeneous pieces of evidence to be combined, which would effectively cause an uncontrolled increase in uncertainty, particularly in the conflict mass, incorporated by combining evidence from different phases. Such a conflict mass does not constitute a useful metric since it is instigated by pieces of evidence which refer to different phases, and hence different hypothesis spaces. DST will accommodate this conflict mass through normalization and therefore will produce inconsistent results. Instead, TBM will reveal the conflict mass but the result will not be aligned with the ground truth. It is impossible to distinguish whether the derived conflict mass is created by truly conflicting evidence referring to the same FoD or by heterogeneous pieces of evidence which refer to different FoD's. Therefore, it is impossible to employ traditional fusion theories in a multi-phase problem' since these theories are 'agnostic' towards this type of scenario.

III. THE MARKOV MULTI-PHASE TRANSFERABLE BELIEF MODEL

This section presents the Markov Multi-phase Transferable Belief Model (MM-TBM) designed to accommodate the detection, tracking and prediction of XAPTs. It employs a tree structure for modelling an attacker's behavior across all phases of an XAPT kill-chain. MM-TBM uses Smets' TBM [17] as its starting point to develop a new and more generalized approach to deal with complex, multi-phased attack vectors that standard TBM treatment cannot address. Incumbent to MM-TBM is the utilization of the associated conflict mass for managing and negotiating paradoxes across the phases of the kill-chain.

A. XAPTs AS MARKOV PROCESSES

A Markov process is a stochastic modelling technique which generates sequences of events in which the probability of an event depends only on the previous event. Sequences which are consistent with this statement are satisfying the Markov property: The future state H_{n+1} of a discrete time Markov process in time $n+1$ is dependent only upon the current state H_n and not on any of the previous states $(H_1, H_2, \ldots, H_{n-2}, H_{n-1})$. Transitioning between each state is associated with a probability mass. Hence, the kill-chain model within the context of XAPTs satisfies the Markov property; the ensuing actions of an attacker are determined by the outcome of the current ones. This is illustrated with the following example: With reference to Fig.1, the

FIGURE 1. The XAPT kill-chain model.

Reconnaissance phase will reveal the target network's vulnerabilities and entry points. The Insertion phase will attempt a breach at the discovered weaknesses by specially crafted malware. The Exploitation phase involves the establishment of the attacker's presence on the target using the tools that were implemented in the Insertion phase. The Target Identification phase involves the control traffic from the attacker's location and the movement within the target network. This communication channel is maintained through the malware employed within the Exploitation phase. During the Exfiltration phase, data is uploaded to an attacker's server; this data was located and identified during the Target Identification phase.

According to the outcome of each phase, attackers may select from a pool of available actions to proceed with their mission, based on the properties of the target network, such as software vulnerabilities, security policies and countermeasures, network architecture, operating systems, network services and the location of the valuable data to be exfiltrated. The likelihood of an attacker's future actions can be estimated with knowledge of prior beliefs.

Markov models are ideal for modelling discrete or continuous-time state transitions of a stochastic process. They are commonly expressed as graphs, in order to illustrate the interdependency among the states.

B. ATTACK TREE

The MM-TBM algorithm employs an attack tree for modelling an adversary's actions towards exfiltrating data from a High Value Target (HVT) within a computer network. We view the Attack tree as a probabilistic network where nodes represent events associated with probabilities or beliefs and edges represent causal links between the events [65]. A concise definition of the attack tree is presented in (1) and a graphical representation of an attack tree, based on (1) is given in Fig.2.

Definition: Let H denote a set of nodes that represent potential attack steps of an XAPT against and HVT. Given i the index of the node, $N(i)$ the name of the node with index $i = 1$, $Par(i)$ the parent node of $N(i)$ and $Pr(i)$ the prior belief associated with $N(i)$, this tree H is an Attack tree with nodes H_i defined as:

$$H_i = \{i, N(i), Par(i), Pr(i)\} \tag{1}$$

with $i = [1, m]$, m : the number of nodes.

The tree structure models all the likely attack paths that an adversary will follow during an XAPT. A node corresponds to the attacker's action that forms an attack phase. The children of a given node represent the plausible hypotheses with respect to the subsequent phases of the attack. $Pr(i)$ represents the belief mass allocated to a node given that the parent node has been confirmed by the evidence i.e. the likelihood that the attack will follow a certain path given an attack phase has been completed.

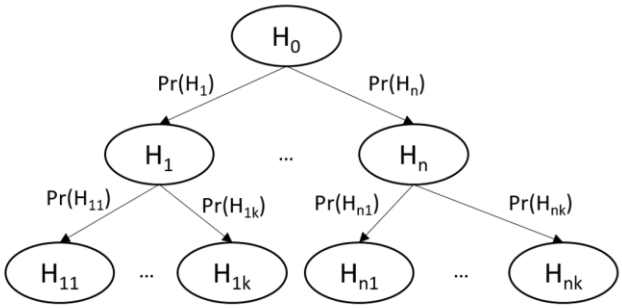

FIGURE 2. Attack tree.

C. HYPOTHESIS ASSESSMENT - THE ALERT AND AWARENESS FRAMES OF DISCERNMENT

MM-TBM incorporates two levels of knowledge for facilitating the monitoring of current malicious activities and enabling prediction for future actions. These two levels are represented by two frames of discernment, namely Alert frame (Ω_{Al}) and Awareness frame (Ω_{Aw}).

The Alert frame contains the actions associated with the next attack phase. It is made up of the children of the nodes that have been supported by the evidence intercepted in the current phase.

Alert Frame Definition: Let p_c denote the current phase of the attack, X the Attack tree, $\Omega_{al}(p_c)$ the current Alert frame and $I_{p_{c-1}}$ the collection of the nodes that have been supported by the evidence in phase $p_c - 1$. The Alert frame is defined by (2).

$$\Omega_{al}(p) = \left\{H_a : Par(a) \in I_{p_c-1}\right\} \tag{2}$$

The Awareness frame Ω_{aw} represents the attacker's potential courses of action to complete an XAPT against one or more HVTs within the protected computer network. Each distinct path of the Attack tree, from the root to each of the leaf nodes becomes a member of Ω_{aw}.

Awareness Frame Definition: Assume a tree H with k leaf nodes, with $J = (j_1, j_2, \ldots, j_k)$ the set that contains the identities of these nodes. The Awareness frame in phase p is defined as:

$$\Omega_{aw}(p) = [H_1, \ldots, H_{j1}], [H_1, \ldots, H_{j2}], \ldots, [H_1, \ldots, H_{jm}] \tag{3}$$

with $1 \leq m \leq k$.

D. COMBINING EVIDENCE - THE MULTIPHASE COMBINATION RULE WITH RESET (MCR^2)

The evidence from the network sensors relevant to Ω_{Al} is converted into basic belief masses. The conversion is made according to pre-defined rules trained based on the sensors' credibility and assessed according to previous evaluation of

the sensors, manufacturer's specifications and shared intelligence. The combination of evidence in MM-TBM is performed by employing the Multi-phase Combination Rule with Reset (MCR^2). This is a novel rule for multi-phased fusion problems which cannot be addressed by Smets' combination rule. The formal proof for MCR^2 is presented below.

The combination of evidence using Smets' combination rule is an iterative process. For n sources of evidence (which are represented by n sets of basic belief masses $m(.)$), $n-1$ combinations are required. Given a frame of discernment Ω, the corresponding power set 2^Ω and two pieces of evidence m_1 and m_2 which refer to 2^Ω, Smets' combination rule is:

$$m(X) = \sum_{A\cap B=X} m_1(A)m_2(B), \quad \forall A, B, X \in 2^\Omega \tag{4}$$

MCR^2 Formal Proof: Consider a tree structure that models the potential paths of an XAPT against a specific computer network. Let $\mathbf{p}$ *the current phase,* $\mathbf{\Omega}$ *the current frame of discernment,* $\mathbf{2^\Omega}$ *the power set and the number of sources of evidence n that generate sets of beliefs* $(m_1, m_2, \ldots m_n)$.

When new sets of beliefs $(m_1, m_2, \ldots, m_n)$ are received the fused belief for each member of the power set 2^Ω is calculated by using Smets' combination rule. Let $z = |2^\Omega|$, then $2^\Omega = \{H_1, H_2, \ldots, H_z\}$. The fused belief for H_i using the conventional Smets' rule, is calculated by iteratively fusing the pieces of evidence:

$$m_{1,\ldots,n}(H_1) = \sum_{A\cap B=H_1} m_{1,\ldots,n-1}(A)m_n(B) \quad \forall A, B, H_1 \in 2^\Omega \tag{5}$$

If (3) is true, then for all hypotheses $H_{1,\ldots,n}, i = [2^\Omega]$, it follows that:

$$m_{1,\ldots,n}(H_i) = \sum_{A\cap B=H_i} m_{1,\ldots,n-1}(A)m_n(B) \quad \forall A, B, H_i \in 2^\Omega, \quad i = [1, 2^\Omega] \tag{6}$$

Equation (6) is an alternative interpretation of Smets' rule. In a multi-phased fusion problem, the above rule must be applied across all the phases, to ensure that the per-phase relevant evidence is fused.

In addition, when the combinations for phase $p-1$ are completed and a new $\Omega_{al}(p)$ is selected, $m_p(\varnothing)$ refers to a new hypothesis space hence is reset to zero. This paper introduces a new operator $(\varnothing) \leftarrow 0$ called the conflict mass reset operator for resetting the conflict mass of the previous phase $(m^{p-1}(\varnothing))$ to 0 when a new Alert frame is selected.

Let $\boldsymbol{C^p}$ *be a body of evidence which contains a number of evidence sources across* $\mathbf{p}$ phases with corresponding pieces of evidence m_i^p.

In order to combine the evidence sources in C^p across all the p phases and to represent the conflict mass reset during the transition from phase $p-1$ to p, (6) is generalised to:

$$m^p_{1,\ldots,n}(H_i^p) \underset{m_p(\varnothing)\leftarrow 0}{=} \sum_{A\cap B=H_i^p} m^p_{1,\ldots,n-1}(A)m^p_n(B), \quad \forall A, B, H_i^p \in 2^{\Omega_{al}(p)}, \quad i = [1, 2^\Omega] \tag{7}$$

Finally, the rule is further generalised to represent any binary combination of sources of evidence within a multi-phased TBM context and is concisely presented for the first time:

$$m^p_{1,\ldots,n} = m^p_{1,\ldots,n-1} \bigoplus_{m^{p-1}(\varnothing)\leftarrow 0} m^p_n \quad \forall\, C^p, n \leq 2 \tag{8}$$

The symbol $\bigoplus_{m^{p-1}(\varnothing)\leftarrow 0}$ denoted in (8) is the novel MCR^2 operator which is an extension to Smets' conjunctive operator [66]. The distinction of the MCR^2 operator is that any conflict mass generated by the combination is reset with every transition to the next Alert frame. Equation 7 is the **analytical form** and (8) is the **general form** of the Multi-phase Combination Rule with Reset (MCR^2). The MCR^2 combination rule yields two outputs:

1) The combined beliefs in respect of the current Alert frame (Ω_{al}).
2) The conflict mass generated for the current Alert frame (Ω_{al})

As soon as all the pieces of evidence have been fused, the outputs are converted to pignistic probabilities using Smets' Pignistic Transformation (see (9)). These probability values are used for updating the prior beliefs associated with each hypothesis represented upon the tree as a node H_i hence $Pr(i) = BetP[H_i]$. Effectively, the new prior beliefs are assigned to their corresponding nodes on the tree, expressing the revised likelihoods for the future events, given the most recent evidence. The bias caused by prior beliefs is thus eliminated and prediction of future events relies on up-to-date information regarding attack status.

$$BetP[H_i] = \sum_{A\subseteq\Omega_{al}(p)} \frac{|H(i)\cap A|}{|A|}\frac{m(A)}{1-m^p(\varnothing)} \quad \forall H(i) \notin \Omega_{al}(p) \tag{9}$$

We consider this novel extension to be along the same lines of [17] upon the Dempster-Shafer theory [16], particularly to the generalization of Dempster's rule of combination by means of Smets' conjunctive rule. Similarly, we consider the MCR^2 to serve as a generalization of the conjunctive rule for multiple, causally linked frames of discernment.

E. PREDICTION OF FUTURE ATTACK STEPS

In accordance with belief updating defined in section III-C, we now proceed with calculating the joint beliefs of the Attack tree paths. To calculate the joint belief or predicted belief $(m_{predicted})$ for each member of the Awareness frame, the beliefs associated with each node from root to leaf are multiplied. The predicted belief of each path represents the

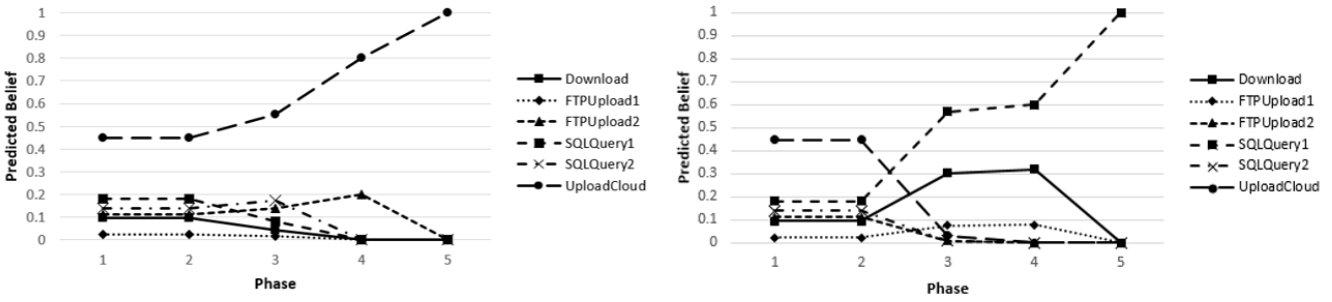

FIGURE 3. Limited objectives experiment predicted belief plots.

likelihood of each outcome of in the Awareness frame as previously specified in (3).

Prediction Formula Definition: Assume an Attack tree H with k leaf nodes. A pathway of the tree consisting of m nodes starting from the root until a leaf node H_{leaf} is reached, is defined as *Path*. The predicted belief for each *Path* is given by the following formula:

$$m_{predicted}(Path) = \prod_{i=(1,m)} Pr(i) \tag{10}$$

F. TREE PRUNING

The prior beliefs of the attack tree nodes are updated based on received and relevant pieces of evidence which are generated during each phase. If the evidence yields zero *BetP* to a node, that node and its descendants represent implausible events and implausible attack paths respectively. Therefore, retaining a zero *BetP* node and its descendants causes redundant information to remain in scope and infers unnecessary noise. The algorithm should, therefore incorporate a functionality for removing implausible hypothesis based on the evidence.

A limited objectives experiment was conducted in order to explore tree pruning within an MM-TBM approach. It involved six use cases, whereby each case assessed an exfiltration attack which followed a certain path across the attack tree. During this experiment, the nodes which were assigned zero *BetP* by the evidence were removed, which includes their descendants i.e. the corresponding subtree. Fig.3 shows the evolution of the predicted beliefs of competing attack paths across the attack phases. The leaf nodes are identified for each attack path in the figure. Inspection of the results shows that, if the $m_{predicted}$ of an attack path declines during an attack phase, eventually $m_{predicted}$ for this attack path becomes zero in a subsequent phase. At the same time, $m_{predicted}$ for ground-truth paths consistently increase across the phases. Therefore, the decision for pruning a path can be made before the phase-relevant evidence presents itself. Based on the empirical evidence and the preceding argument, the rule for removing an attack path is stated as follows:

Let H be an Attack tree that consists of $\boldsymbol{\nu}$ paths, where each path is denoted by $path_j$ where $j = [1, \nu]$. Let $\boldsymbol{p}$ be the number of phases, so that the predicted belief for each $path_j$ at phase i is denoted by $m(path_j^i)$ where $i = [1, p]$. The condition for pruning a path is given in (11):

$$m_{predicted}(path_j^{i-1}) > m_{predicted}(path_j^i) \longrightarrow prune(path_j) \tag{11}$$

Based on this finding, the size and shape of the attack tree can adapt to an attack. As the attack progresses through the kill-chain and more relevant pieces of evidence are intercepted, some of the nodes (and their matching paths) are pruned, causing the tree to reduce in size and the hypothesis space to decrease.

The prior beliefs associated with the remaining nodes of the Alert frame are updated in accordance with the belief updating process described in section III-B. The next Alert frame will consist of the children of the nodes that were allocated a *BetP* at the last combination.

G. DIAGNOSTIC FUNCTIONALITY

In order to handle situations of missing evidence, MM-TBM incorporates a diagnostic functionality for assessing hypotheses which belong to future phases. Effectively, this function is performed by monitoring events which belong to a lower level of the tree, precisely one phase ahead of the current Alert frame. The belief associated with the specified nodes is calculated using the combination rule and the pignistic transformation as in normal operation. In this case however, the derived beliefs enable the revision of the tree state, by employing a bottom-up approach, as opposed to the top-bottom approach applied during normal operation.

Diagnostic Formula Proof: Let us consider a Bayesian network with hypotheses $(H_1, H_2, \ldots, H_n)$*, the body of evidence e and the conditional probabilities* $P(e|H_1)$*,* $P(e|H_2)$ *to* $P(e|H_n)$.

The Bayesian rule states that:

$$P(H_i|e) = \frac{P(e|H_i)P(H_i)}{P(e|H_1)P(H_1) + \ldots + P(e|H_n)P(H_n)} \tag{12}$$

With $i = [1, n]$.

Provided that $P(H_1|e) + P(H_2|e) + \ldots + P(H_n|e) = 1$.

The Bayesian rule can be expanded to directed acyclic graphs, such as the Attack tree within the context of MM-TBM. Assume the tree structure in Fig.4, whereby

hypothesis H_0 has been supported by evidence, $\Omega_{al} = [H_1, \ldots, H_n]$ and the prior beliefs of the nodes are denoted by $Pr(.)$.

Let us assume that the new incoming evidence is associated with the leaf nodes and not with the current Ω_{al}. The pignistic probabilities calculated from the evidence can be used to update the prior beliefs for their respective branches $[Pr(H_{11}), Pr(H_{12}), \ldots, Pr(H_{nk})]$. However, the prior beliefs of the hypotheses within the Alert frame must also be updated $[Pr(H_1), \ldots, Pr(H_n)]$, to ensure that the joint probability of each path is calculated based only on the observed evidence and by omitting any pre-assigned prior beliefs. Due to missing evidence with respect to the hypotheses of the Alert frame, the evidence which is relevant to the Next Alert frame denoted as $\Omega_{N_{al}} = [H_{11}, \ldots, H_{1k}, \ldots, H_{nk}]$ is the only source of useful information. Hence, for every hypothesis in the leaf nodes the prior beliefs are updated as follows:

$$Pr(H_{ij}) = BetP(e_{ij}|H_i)$$

where $i = [1, n], j = [1, k]$ and $e_{ij} = H_{ij}$.

It is also known that:

$$\sum_{i=[1,n],j=[1,k]} BetP(H_i|e_{ij}) = 1 \tag{13}$$

The pignistic probability for each member of $\Omega_{N_{al}}$ is given by:

$$BetP(e_i|H_i) = \sum_{j=[1,k]} BetP(e_{ij}|H_i) \quad \forall i \in [1, n] \tag{14}$$

where $e_i = [e_{i1}, e_{i2}, \ldots, e_{ik}]$ By combining (12) with (13), it follows that:

$$BetP(H_i|e) = \frac{BetP(e_i|H_i)Pr(H_i)}{BetP(e_1|H_1)Pr(H_1) + \ldots + BetP(e_n|H_n)Pr(H_n)} \tag{15}$$

By combining (14) with (15), it follows that:

$$BetP(H_i|e) = \frac{Pr(H_i)\sum_{j=1}^{k} BetP(e_{ij}|H_i)}{\sum_{i=1}^{n}[Pr(H_i)\sum_{j=1}^{k} BetP(e_{ij}|H_i)]} \quad \forall i \in [1, n] \tag{16}$$

which is MM-TBM's diagnostic formula.

H. TREE SLICING

XAPTs may originate from different adversaries at the same time. It is therefore necessary to develop a mechanism for detecting the presence of concurrent multiple attacks within the network. In order to address this class of problems, a Tree slicing function has been developed. This function creates slices of the tree which track each individual attack path that is occurring in parallel with additional attacks.

The slices are generated when the conflict mass computed by the MCR^2 is greater than zero. When $m(\varnothing) > 0$, the tree is sliced at the portion that was referring to the last known Alert frame. The number of the new tree slices is equal to $|\Omega_{al}|$.

Let X be an Attack tree, the current Alert frame Ω_{al} and x_n the members of Ω_{al} with $n = [1, |\Omega_{al}|]$. If the combination of evidence results in $m_{\Omega_{al}}(\varnothing) > 0$ then the tree X will be divided into n slices.

Each new slice will contain the following: 1) one member of the Alert Frame, 2) its predecessors and 3) its descendants. An illustration of a Tree slicing is illustrated in Fig. 4. The n slices are generated when $\Omega_{al} = [H_1, H_n]$. After the split, each slice is tracked individually as an independent Attack tree, using the same pool of evidence but focusing on the subset of evidence which is relevant, as defined by the Alert Frame.

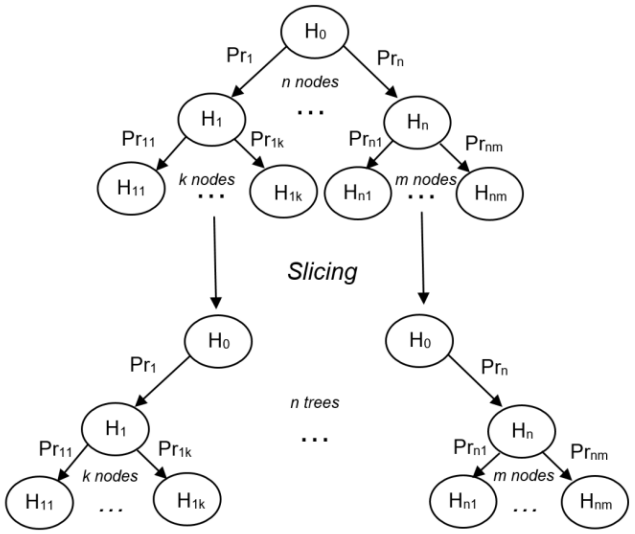

FIGURE 4. Attack tree before and after slicing on nodes H_1 and H_2.

I. MCR^2 v SMETS' RULE: A CONCRETE ILLUSTRATION

Lofti Zadeh [50] showed that Dempster's rule of combination results in misleading and counterintuitive conclusions when disagreement between sources of evidence is very high. In a similar way, we illustrate by the following example that Smets' rule of combination cannot cope with situations where pieces of evidence refer to multiple and disjoint frames of discernment.

Consider a fusion problem which is concerned with a dual-phase process. In order for the second phase to materialize, it is mandatory that the first phase is completed. In the first phase, the potential events are $\{A_1, A_2, A_3\}$. In the second phase, the potential events are $\{B_1, B_2, B_3\}$. In order to track the specified process, the events of both phases must be intercepted, reported by the sources of evidence and combined accordingly. There are two available sensors for phase 1 and two sensors for phase 2 which are labelled as m_{a1}, m_{a2}, m_{b1} and m_{b2} respectively. Table 1 contains the measurements from the four sensors. The combinations are performed by using

TABLE 1. Sensor outputs.

Sensor	A_1	A_1, A_2, A_3	B_1	B_1, B_2, B_3
m_{a1}	0.6	0.4	0	0
m_{a2}	0.7	0.3	0	0
m_{b1}	0	0	0.8	0.2
m_{b1}	0	0	0.6	0.4

MCR^2 (7) and Smets' combination rule [17]. The results are given in Table 2.

Using the Smets' rule the sources of evidence are not combined in accordance to the mutual-exclusivity property, hence the value of the conflict mass becomes unity, which does not allow any kind of inference or decision. On the other hand, the MCR^2 is applied within an appropriate hypothesis assessment, whereby the observed process is decomposed into its constituent phases and two frames of discernment that follow the mutual exclusivity property are constructed.

The results of MCR^2 provide a clear winner in both phases, namely A_1 and B_1 respectively. This example shows that TBM as well as conventional single-phase techniques such as Dempster-Shafer theory are inadequate for handling multi-phase fusion problems as opposed to MM-TBM, which is designed for this specific class of problems and utilizes a combination rule for representing the transition between phases including the reset of the associated conflict mass.

IV. SCENARIO AND EXPERIMENTAL DESIGN

This section describes the scenario design for developing and validating the MM-TBM approach through a number of experiments. The scenario and experimental designs were validated by Subject Matter Experts from the UK's Defense and Science Technology Laboratory. This section describes the Main experiment and evaluation of MM-TBM. The objectives of the Main experiment are to:

1) Assess the performance of MM-TBM.
2) Identify the limits and optimal operational parameters of MM-TBM with reference to sampling of the alert database.

At first, we defined three experimental Vignettes for assessing key functionalities of MM-TBM. A computer network for recreating a number of XAPT kill-chains was developed as the experimental setup within the experimental design. This setup influenced the design of an Attack tree that maps the potential kill-chains that could be presented in the computer network. To comply with the Concept of Employment for developing new Cyber SA capabilities [8], we incorporated the five characteristics of the cyberspace (*Contested, Congested, Cluttered, Connected, Constrained*). More details with regards to the conformity of the scenario design to the cyberspace characteristics are given in Table 3.

In our approach, the attack tree-driven hypothesis assessment scheme creates Alert frames of discernment based on the attack's state and fuses the relevant evidence using the MCR^2 combination rule. Consequently, the scope of the algorithm is constantly focused on the state of the attack and is permitted to consider only a subset of the evidence presented. Assuming that an XAPT will create zones of relevant evidence within the alert log, where each zone will correspond to an attack phase, identification of these zones becomes a challenge. The question remains however, as to how many of the alerts should be allocated at each time in order to identify and combine relevant pieces of evidence. Since the interval between attack phases is unknown, how can one decide how many alerts to allocate in a sample of the alert log to: 1) isolate the ground-truth from clutter as much as possible; 2) contain precisely one phase in a sample and; 3) prevent the evidence of an attack phase from being divided into two or more consecutive samples?

To investigate the implications of choosing various sampling sizes, we utilize several different sampling periods, based on the timestamps of the alerts. The results produced by each sampling period are compared using the Kruskal-Wallis and Nemenyi tests to identify the optimal sampling strategy for MM-TBM within the experimental scenario.

A. VIGNETTES

To evaluate the functionality of MM-TBM, a set of scenarios to test this functionality were developed in accordance with the evidence presented during each attack phase of the Cyber Kill Chain. These scenarios are divided into three Vignettes (categories).

The set of scenarios under Vignette V1 test how MM-TBM responds to multi-phased XAPTs by means of assessing the

TABLE 2. Belief masses after combination.

	A_1	A_2	A_3	A_1, A_2	A_1, A_3	A_2, A_3	Ω_A	B_1	B_2	B_3	B_1, B_2	B_1, B_3	B_2, B_3	Ω_B	$\varnothing$
MCR^2 Phase 1	**0.88**	0	0	0	0	0	**0.12**	0	0	0	0	0	0	0	0
MCR^2 Phase 2	0	0	0	0	0	0	0	**0.92**	0	0	0	0	0	**0.08**	0
TBM Phases 1 & 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**

TABLE 3. Scenario design compliance.

Characteristic [8]	Description	Scenario Design Compliance
Contested	No one individual, organization or nation controls access to, and freedom of action within, cyberspace. Cyberspace in itself is no respecter of hierarchy or the level of user, indeed its freedom of use is its attraction.	MM-TBM is designed to operate as a control mechanism for tracking and predicting multi-phase cyber-attacks in the cyberspace.
Connected	Cyberspace is rapidly becoming the 'common' global common, with complex and adaptive networks constantly evolving on a local, regional and global scale. These networks are potentially available to anyone with access; amorphous with no obvious leader/hierarchy.	Experiments are conducted in a cyber range that simulates a 'connected' cyberspace. The scenarios simulate situations where an attack propagates from the Internet to High Valued Targets within the network.
Congested	Individuals, organizations and nations have been drawn into using technologies and systems that almost totally rely on access to cyberspace. Network limitations and constraints may create the impression of congestion.	The scenario design tests the effect of congestion in MM-TBM's operation.
Cluttered	Cyberspace enables anonymity, making it difficult to determine the source of incidents and to discriminate between malicious and individual or organizational negligence.	The scenario design tests the effect of clutter (Low, Medium, High) in MM-TBM's operation.
Constrained	There is an increasing need for common principles, understanding and norms of behavior to be established amongst stakeholders and users to address the security issues that arise from the conduct of activity in and through cyberspace.	This characteristic is concerned with the legal constraints of cyberspace and is outside the scope of the scenario design.

TABLE 4. Attack vectors.

Vulnerability	Exploit name
(N/A)	Nmap scanner
CVE-1999-0506	MSSQL Login Utility
CVE-2000-0402	Microsoft SQL Server Payload Execution
CVE-2000-1209	Microsoft SQL Server Payload Execution via SQL Injection
CVE-2005-2611	Veritas Backup Exec Windows Remote File Access
CVE-2008-4250	Microsoft Server Service Relative Path Stack Corruption (MS08-067)
CVE-2009-3103	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference (MS09-050)
CVE-2011-4828	V-CMS PHP File Upload and Execute
CVE-2012-1823	PHP CGI Argument Injection
CVE-2012-1465	NetDecision 4.5.1 HTTP Server Buffer Overflow
CVE-2013-0632	Adobe ColdFusion 9 Administrative Login Bypass
CVE-2013-4212	Apache Roller OGNL Injection
CVE-2014-0050	Apache Commons FileUpload and Apache Tomcat DoS

Hypothesis Assessment, MCR^2, Prediction and Tree Pruning functionalities (Sections III-C to F). Vignette V2 contains scenarios where an attack phase is not intercepted, so that we could additionally test the Diagnostic functionality

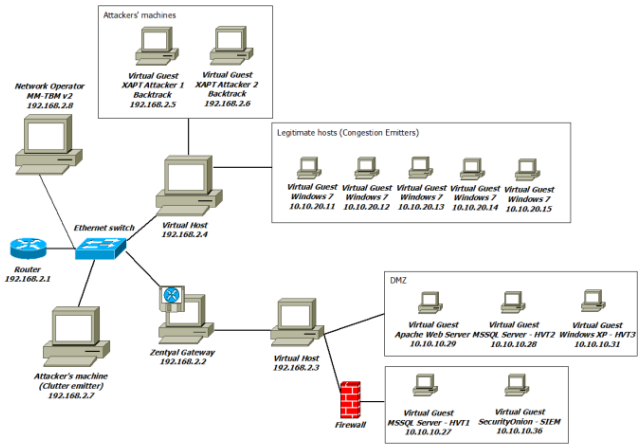

FIGURE 5. Cyber range network topology.

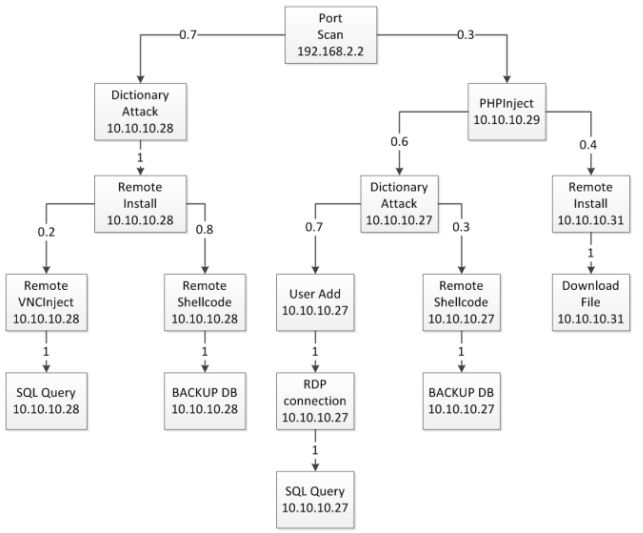

FIGURE 6. Attack tree.

(Section III-G). In Vignette V3, we were concerned with MM-TBM's capacity to detect two concurrent XAPTs hence evaluate the Tree slicing functionality (Section III-H). The Vignettes are illustrated in Table 5.

B. NETWORK TOPOLOGY

The experiments were conducted in a controlled computer network environment. The network topology of the environment is given in Fig.5. There are three target machines (two Windows 2008 R2 servers with Microsoft SQL Server 2012 and one Windows XP machine). One server is protected by Zentyal firewall whereas the remaining two targets are in the Demilitarized Zone. Five stations are used for generating legitimate traffic by issuing SQL queries against the database servers and HTTP GET requests at an Apache web server. With reference to the vignettes, the attackers seek to exfiltrate data by 1) submitting SQL queries to a database server, 2) downloading database backup files through FTP

TABLE 5. Vignettes.

ID	DESCRIPTION	No of scenarios	Scenario ID's
V1	An attacker launches an XAPT against an HVT within the LAN	5	V1s1, V1s2, V1s3, V1s4, V1s5
V2	An attacker launches an XAPT against an HVT within the LAN. The evidence in a phase of the attack kill-chain is missing.	3	V2s1, V2s2, V2s3
V3	Two attackers launch XAPT attacks against two HVTs within the LAN.	3	V3s1, V3s2, V3s3

and 3) by downloading sensitive files from a commander's workstation.

C. ATTACK TREE

For the purpose of this paper, the Attack tree structure and prior beliefs have been co-designed with Subject Matter Experts from Airbus and the Defense and Science Technology Laboratory. The tree models the potential attack pathways of an adversary during an XAPT mission against the designated High Valued Targets. Each node corresponds to a specific attack vector against a given network station and the branches are labelled with the prior beliefs associated with the corresponding node.

Various approaches and techniques exist for designing attack graphs and training prior probabilities (see [63], [64] for a detailed review). The attack tree for the experiment presented in this paper (Fig.6) is designed based on the network topology, the operating systems and the installed services and applications of the controlled computer network environment (see Section II-B). The data exfiltration targets are selected servers or workstations where critical information is preserved and constitute the High Valued Targets of the reference network. By focusing on the most valuable assets, the attack surface and potential multi-step paths across the network can be assessed through red-team/blue-team exercises [65]. Hence, the search space for potential attack paths is much reduced and tractable. Moreover, as HVT's are commonly located deep within the network and are accessible only from a limited number of network components (i.e. through a web-application firewall), there are very few routes available for an adversary to reach their target.

This design approach is good for building a knowledge-base of potential attacks for multi-phase detection which is robust to false positives but is nevertheless limited in addressing alternative attack routes or zero-day attacks [64] which a ''smarter'' attacker may employ. MM-TBM is designed to address the effects of zero-day attack vectors by means of the diagnostic functionality. Zero-day attacks may not be traced because a matching signature has not been incorporated in the IDS or any other signature-based detection scheme. Even in the absence of the appropriate signature, MM-TBM can accommodate evidence of any kind, such as anomaly detectors or log management tools where a zero-day attack may leave a matching trail.

Similarly, an XAPT may follow a path that is not represented on the Attack tree either because of a non-exhaustive assessment of attack paths, or because a zero-day attack made it possible to follow alternative routes. In this case, the diagnostic functionality can resolve attack paths that follow alternative routes provided that the attacker's path converges to the tree-prescribed path after a phase. Nevertheless, there is always a chance that a zero-day attack will follow an attack path that is not represented on the Attack tree and therefore completes without being detected. This is a case that the MM-TBM will not manage, however the post-incident forensic analysis will help reveal the undetected path which can then be incorporated into the Attack tree.

D. DATA GENERATION AND COLLECTION

The XAPT attacks as well as the clutter traffic (see next paragraph) were launched from an attacker's station running the Kali Linux operating system. The exploits used for running the experiments are given in Table 4. When these attacks were launched, they were detected by the Security Onion SIEM and generated IDS alerts and Windows Log entries which were stored in a MySQL database. The alert log created by an attack scenario forms the dataset for the respective scenario. The experiments are conducted in the presence of legitimate background traffic and spurious attacks which may or may not be relevant to the Attack tree nodes (hereby called *clutter*). Three types of clutter are introduced in order to confuse the algorithm into committing to false hypotheses within an attack phase. In Low clutter, the attack scenario was launched alongside constantly emitted legitimate background traffic and spurious attacks that generated evidence which was not relevant to any of the hypotheses represented on the attack tree, and therefore deemed out of scope. In Medium clutter conditions, the same attacks were launched as in Low clutter, plus a constantly emitted attack which corresponds to a single node of the attack tree. In High clutter conditions, the same attacks were launched as in Low clutter, plus repeatedly emitted two or three attack phases; these correspond to partial attack paths along the tree. It is anticipated that Low clutter shall have zero effect on MM-TBM performance. Regarding Medium clutter, it is expected that the algorithm will detect a false phase and cause the tree to slice (according to the Tree slicing functionality described in Section III-H). With reference to High clutter, it is expected that the algorithm

will detect at least one false phase, create a slice and track a bogus path. Within this cluttered network environment, the experiment evaluates how the MM-TBM can cope with various adverse conditions that may be realized in an actual XAPT.

Each of the 11 scenarios (See Table 5) is executed three times, one for each type of clutter, resulting in a total of $3 \times 11 = 33$ datasets. Each of these datasets is processed by MM-TBM with 7 different sampling periods. The alerts contained in the dataset are converted to basic belief assignments using pre-defined lookup tables. The dataset contains 60 seconds of collected alerts generated before the 1st phase of the XAPT is launched. An interval of 60 seconds is kept between each attack phase to ensure that they are kept distinct. Background traffic is generated constantly during the experiment and the corresponding alerts are populated in the alert table. The generated dataset contains three columns: *signature_id*, *timestamp* and *dst_ip* since these are the features that are used for generating the belief assignments. The table entries are then divided into a number of segments for processing.

Seven different periods are used for segmenting the alerts, namely: 30, 45, 60, 75, 90, 105 and 120 seconds. These values have been set to straddle the phase separation time of 60 seconds. An alert table with r number of entries is divided into a number of segments, based on the values of the timestamp column. Each segment contains the entries $[r(t_n), r(t_{n+1})]$, where $t_{n+1} - t_0 = sample\ period$. The last segment contains the entries $[r(t_n), r_{end}]$ where r_{end} denotes the last entry. $|seg|$ denotes the number of segments produced for each sampling period.

The algorithm is executed once for each dataset and for $|seg|$ iterations, processing each segment sequentially. If the pieces of evidence located in the current segment are relevant to the current *Alert* or Next Alert frames, then these pieces of evidence are processed and utilized for updating the tree. If no relevant evidence is detected, the segment is discarded (See Fig.7 for algorithm pseudocode).

Algorithm MM-TBM (X, e)

```
//Where X the Attack tree and e the latest evidence
phase = 1;
while (e ≠ null) do
    get_frames(X);
    if e ∉ e(Ω_al)
        if e ∉ e(Ω_al)
            collect_new evidence();
            continue;
        else
            MCR²(X, e);
            Diagnostic_rule(X);
            prune_tree(X);
            collect_new_evidence();
            phase = phase + 2;
            continue;
        end if
    else
        MCR²(X, e);
        if m(Ø) > 0
            slice_tree(X);
            collect_new_evidence();
            phase = phase + 1;
            continue;

        else
            prune_tree(X);
            collect_new_evidence();
            phase = phase + 1;
            continue;
        end if
end if
end while
Return X;
```

FIGURE 7. MM-TBM Pseudo algorithm.

E. STATISTICAL ANALYSIS AND CYBER SA EVALUATION APPROACH

This experiment utilizes a set of variables which are adapted from the SA metrics proposed by [45]. These variables are used to measure the Situational Awareness of MM-TBM users by comparing the algorithm output to the ground truth at each phase of the XAPT. Table 7 contains the definition of the variables.

The Phase Recall (PR) values represent the algorithm's capability to efficiently track the XAPT across the phases. Therefore, high Phase Recall indicates that the XAPT attack phases are tracked and predicted with high accuracy whereas low Phase Recall indicates that some ground truth phases are missed. The Phase Precision (PP) values represent the effect of noise caused by legitimate traffic and clutter in tracking the attack phases. When Phase Precision is high, the detected attack phases correspond to the ground truth. On the other hand, if Phase Precision is low, a large number of phase detections are a consequence of clutter, instead of the ground truth.

Similarly, Evidence Recall (ER) represents the capability to focus on the relevant evidence. High Evidence Recall values indicates that the pieces of evidence processed by MM-TBM were indeed part of the ground truth whereas low values show that the relevant pieces of evidence were missed. Evidence Precision (EP) represents the algorithm's efficiency in distinguishing the ground truth evidence from noise. Therefore, high Evidence Precision values indicate that the pieces of evidence that MM-TBM combined were relevant to the ground truth, whereas low values indicated that a high number of evidence processed were generated by clutter traffic. The above metrics are used to assess the effects of utilizing the various sampling periods. The first part of the analysis is concerned with picking out the optimal sampling period using the Kruskal-Wallis test (due to the non-Gaussian distribution of the data). This is a non-parametric statistical test for measuring statistically significant differences among groups. Further, the Nemenyi post-hoc test reveals which of the significantly different groups, at the $p < 0.01$ level are the best performers for the experiments.

TABLE 6. Clutter conditions.

Type	Description
Low	Spurious attacks against various HVTs, outside the scope of the Attack tree.
Medium	Spurious attacks against HVTs, outside the scope of the Attack tree. One attack which corresponds to a phase of the attack tree.
High	Spurious attacks against HVTs, outside the scope of the Attack tree. Two or more attacks which correspond to two or more consecutive phases of the attack tree.

TABLE 7. Experimental performance variables.

Name	Variable
Phase Recall	$\frac{\text{No of Correctly Detected Phases}}{\text{Total No of Phases in the Ground Truth}}$
Phase Precision	$\frac{\text{No of Correctly Detected Phases}}{\text{Total No of Detected Phases}}$
Evidence Recall	$\frac{\text{No of Correctly Detected Alerts}}{\text{Total No of Alerts in the Ground Truth}}$
Evidence Precision	$\frac{\text{No of Correctly Detected Alerts}}{\text{Total No of Detected Alerts}}$

V. RESULTS AND FINDINGS

In this Section, the results and findings of the scenario-based experiments for testing MM-TBM are presented. Firstly, the optimum sampling period for the scenarios is determined using Kruskal-Wallis [59] and Nemenyi [60] hypothesis testing, given the non-Gaussian nature of the data.

Having identified the optimum sampling period, we then evaluate the performance of MM-TBM using the Cyber SA experimental performance variables (Table 7) with respect to identifying the ground truth and distinguishing an XAPT from background clutter and congestion. Lastly, we discuss the benefits and trade-offs associated with an MM-TBM approach for resolving XAPTs.

A. SELECTING THE OPTIMAL SAMPLING PERIOD

Table 8 shows that Phase and Evidence Recall variables produce significantly different results under different sampling periods for *Medium*, *High* and *Overall* clutter for a p value of 0.01. On the other hand, Phase and Evidence Precision variables produce significantly different results under different sampling periods only for Low clutter conditions. Table 9 presents the results of the post-hoc Nemenyi test for identifying the significant differences between the sampling times.

Each cell of Table 9 contains the variables and clutter type for which the sampling period of the cell row produces significantly higher means compared to the sampling period of the cell column. The results show that the best performing sampling period is 90 seconds which maximizes the performance of MM-TBM, i.e. all the means for PR(O, M), ER(O, M, H), EP(L) were significantly higher at the $p < 0.01$ level.

TABLE 8. Kruskal-Wallis test results.

Name	Low	Medium	High	Overall
Phase Recall	0.012	**0.0028**	**0.0023**	**$1.03\text{x}10^{-8}$**
Phase Precision	**$9.46\text{x}10^{-6}$**	0.8691	0.1857	0.1255
Evidence Recall	0.0128	**$8.23\text{x}10^{-4}$**	**$3.41\text{x}10^{-5}$**	**$7.89\text{x}10^{-9}$**
Evidence Precision	**$1.33\text{x}10^{-4}$**	0.9634	0.0178	0.1787

The values in bold indicate that the value is lower than the p = 0.01 threshold, hence a significant contrast among the groups

TABLE 9. Nemenyi post-hoc test results p-value < 0.01.

	Sampling times (in seconds)						
	30	**45**	**60**	**75**	**90**	**105**	**120**
40	-	-	-	-	-	-	-
60	-	-	-	-	-	-	-
75	*PR(O) PR(M) ER(O) ER(M)*	*PR(O) ER(O)*	-	-	-	-	*PR(O)*
90	*PR(O) ER(O) ER(M) ER(H) EP(L)*	*PR(O) ER(O) ER(H)*	*ER(H)*	-	-	-	*PR(O)*
105	*ER(O)*	-	-	-	-	-	-
120	*EP(L) PP(L)*	*PP(L)*	-	-	-	-	-

PP: Phase Precision, EP: Evidence Precision
PR: Phase Recall, ER: Evidence Recall
(L): Low clutter, (M): Medium clutter, (H): High clutter, (O): Overall

Based on the findings, when the sampling period is small, the algorithm becomes more susceptible to losing track of the attack path under Medium and High levels of clutter. On the other hand, sampling at small intervals becomes effective when the clutter is Low. Further, as the sampling period becomes larger, evidence across subsequent phases are more likely to be captured in a single sample hence an attack phase will be missed irrespective of the clutter volume. It follows that MM-TBM delivers best performance when the sampling period is of sufficient duration to capture sufficient evidence. Based on this principle, the optimal sampling period can be dynamically assigned taking into account the characteristics of an attack phase such as the attack vectors and tactics utilized by the adversary. Recent work [63], [64] has shown that the duration of an attack phase can be approximated to a normal distribution. Therefore, an estimation of the attack phase duration is possible and facilitates the dynamic selection of the sampling period to successfully track the subsequent phases.

B. CYBER SA PERFORMANCE

With reference to Fig.8, we observe a number of findings. Phase Recall is high in 85% of the scenarios i.e. the

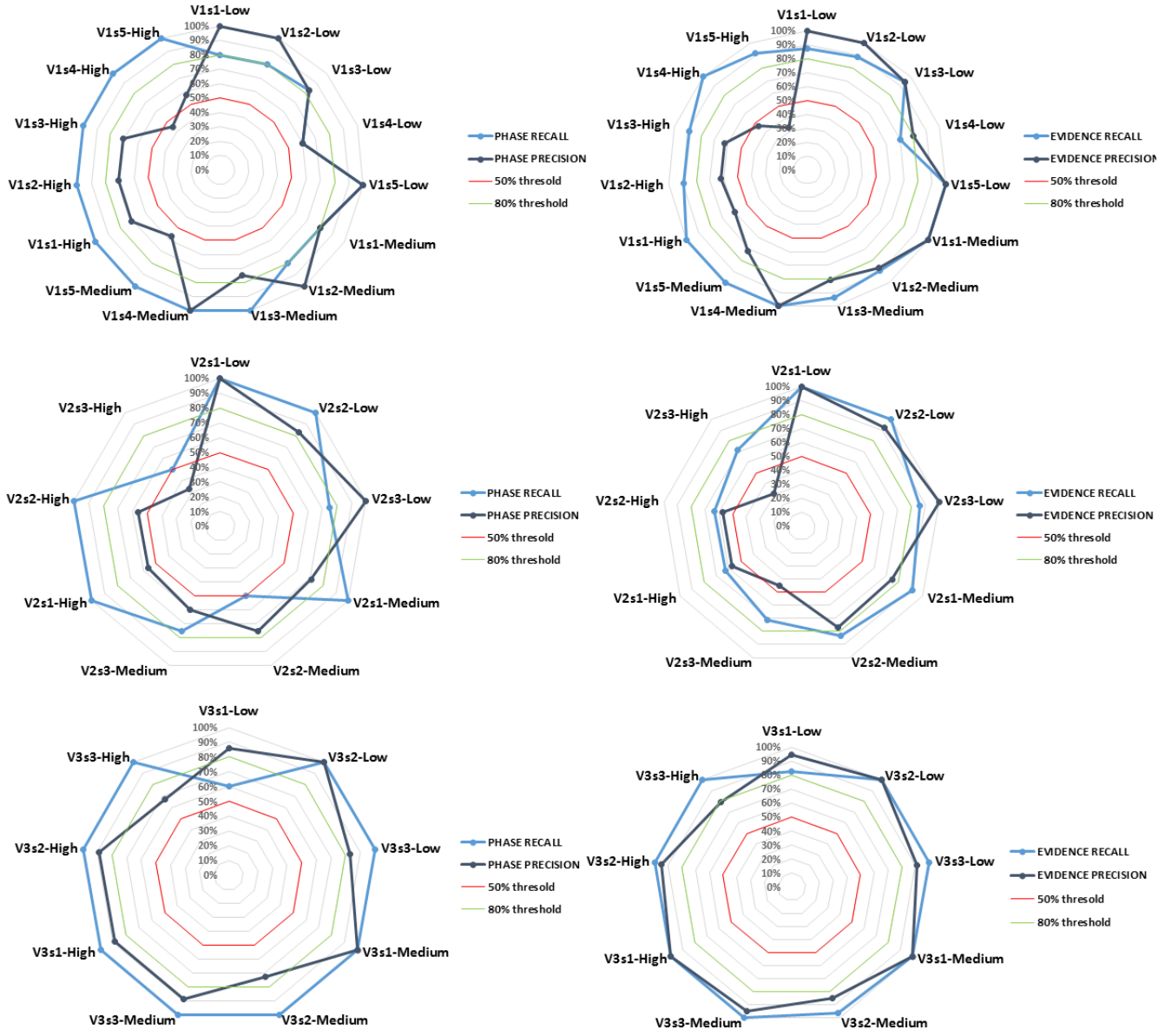

FIGURE 8. Radar diagrams of experimental performance variables in vignettes V1, V2, V3 for Low, Medium, High clutter.

hypothesis space of the awareness frame reduces to a single element when PR $\geq$ 80%. Equally, Evidence Recall is high in 82% of the scenarios, Phase Precision in 52% and Evidence Precision in 63% of the scenarios. The results indicate that the ground-truth phases and evidence are being detected hence the attack is tracked accurately and the future phases remain within scope.

A drop below 80% in Phase and Evidence Recall is observed in V2 results (Fig. 8(c), 8(d)). In these cases, where evidence is missing (see Table 5), MM-TBM dismissed the ground-truth hypothesis within the Alert frame because of clutter and did not manage to track the right path. Nonetheless MM-TBM still achieves high performance over 70% of the time for all the other scenario settings associated with V2, which is still beneficial for cyber SA.

Phase and Evidence Precision values deteriorate under Medium clutter. Clutter traffic triggers more IDS detections hence an increase in the denominator (see Table 7 for the formulae) and the drop in Precision. Medium and High clutter cause the tree to slice (see Tree Slicing functionality, Section III-H) because the MCR^2 yields $m(\varnothing) > 0$. High clutter causes further uncertainty to MM-TBM by forcing it to detect clutter evidence for two or three consecutive phases, effectively tracking a bogus path. The increase in the number of false detections cause a further decrease in Precision (due to the increase in the denominator). Nonetheless, this drop

in Precision is an indication of how MM-TBM copes with uncertainty. In some cases (i.e. V1s4&5-High and V2s1&2-High) we observe large differences between Recall and Precision. These discrepancies occur when the algorithm creates a slice and tracks a bogus path. Given that Phase and Evidence Recall remain high, we infer that the ground-truth path is successfully tracked and predicted despite the high volumes of clutter. Specifically, MM-TBM tolerates false detections to sustain Recall and keep the ground-truth within scope, the trade-off being the drop in Precision. This is an insurance mechanism that prevents the algorithm from committing to a wrong path which is then disposed of when the collected evidence no longer supports it.

The above findings show that the sources of uncertainty are well understood and MM-TBM employs the necessary coping mechanisms, in respect of tree slicing and tree pruning, to deal with these situations. These mechanisms could not be realized without the MCR^2 and the conflict mass reset operator which provide a novel capability for handling uncertainty where multi-phase fusion problems are concerned. In addition, the findings confirm that the scenario design has tested the MM-TBM approach to its functional limits and assisted in determining its optimal operating parameters within an overall approach.

VI. CONCLUSIONS

This paper set out to develop new Cyber SA capabilities and an algorithmic approach for detecting, tracking and predicting XAPTs across the cyber kill-chain. Thus far there has been no theory capable of dealing with the multi-phase nature of cyber-attacks whilst still attending to problems associated with managing conflicting evidence and inherent uncertainty. This new approach, MM-TBM, with its novel combination rule (MCR^2) provides the means to elicit previously indeterminable Cyber SA for complex, multi-phase cyber-attacks.

The MCR^2 (8) with its reset operator is introduced to facilitate management of the conflict mass. This overcomes the inadequacy of Dempster's [16] and Smets' [17] combination rules for multi-phase problems. We have demonstrated MCR^2 allows us to tackle a class of hitherto unresolved problems by proving the Smets' combination rule violates the mutual exclusivity property i.e. $m(\varnothing) = 1$.

With reference to XAPT cyber-attacks, in order to overcome the challenges of a congested, cluttered and contested environment found in practice, MM-TBM employs tree pruning, tree slicing (when $m(\varnothing) > 0$) and the diagnostic functionality as part of the overall control mechanism for effective Cyber SA.

From a practical perspective this research has also demonstrated that sampling time matters to the performance of MM-TBM. Specifically, sampling period should be of sufficient duration to capture sufficient evidence for MM-TBM to deliver best Cyber SA performance. Until now this vital point in the assessment of Cyber SA algorithmic performances has been ignored [33]–[35].

The findings confirm that the scenario design has tested the implementation of MM-TBM to its functional limits. Namely, in terms of overall performance, MM-TBM successfully tracks attack phases over 85% of the time and therefore predicts possible outcomes by reducing the hypothesis space Ω_{Aw} to h at each phase transition such that $h \subset |\Omega_{Aw}|$. This is achieved by utilizing the coping mechanisms (tree slicing and tree pruning) for dealing with clutter whilst compensating for any drop in precision.

In conclusion, we have shown the MM-TBM approach, premised on our MCR^2, is a new Cyber SA capability for addressing previously intractable multi-phase attacks. MM-TBM establishes a fresh perspective for problems where Cyber SA is considered indeterminable and where uncertainty and paradox are a source of unresolved confusion. Furthermore, MM-TBM constitutes a contribution to the field of data fusion with future application to: big data analytics, medical diagnosis, fault detection, forensics, etc. where detection, tracking and prediction is essential for superior SA and decision making.

REFERENCES

[1] CNET. (Jul. 23, 2013). *Cyberattacks account for up to $1 trillion in global losses*. [Online]. Available: https://www.cnet.com/news/cyberattacks-account-for-up-to-1-trillion-in-global-losses
[2] World Economic Forum. (2016). *The Global Risks Report*. 11th ed. [Online]. Available: http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf
[3] F. Zhang, P. P. K. Chan, B. Biggio, D. S. Yeung, and F. Roli, "Adversarial feature selection against evasion attacks," *IEEE Trans. Cybern.*, vol. 46, no. 3, pp. 766–777, Mar. 2016.
[4] T. Moore, "On the harms arising from the Equifax data breach of 2017," *Int. J. Crit. Infrastructure Protection*, vol. 19, no. C, pp. 47–48, Dec. 2017.
[5] J. Keane. Hacked in 2014: The Year of the Data Breach. Paste Magazine, Dec. 2014. [Online]. Available: https://www.pastemagazine.com/articles/2014/12/hacked-in-2014-the-year-of-the-data-breach.html
[6] G. Ioannou, P. Louvieris, N. Clewley, and G. Powell, "A Markov multi-phase transferable belief model: An application for predicting data exfiltration APTs," in *Proc. 16th Int. Conf. Inf. Fus.*, Jul. 2013, pp. 842–849.
[7] C. Tankard, "Persistent threats and how to monitor and deter them," *Netw. Secur.*, vol. 2011, no. 8, pp. 16–19, Aug. 2011.
[8] MNE7. (Feb. 25, 2013). *MNE7 Access to the Global Commons Outcome 3 Cyber Domain Objective 3.5 Cyber Situational Awareness Concept of Employment for Cyber Situational Awareness Within the Global Commons Dated*. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a587471.pdf.
[9] FireEye, "The advanced persistent threat," FireEye, Milpitas, CA, USA, Tech. Rep. M-Trends 2010, Jan. 2010. [Online]. Available: https://www.fireeye.com/blog/threat-research/2010/01/m-trends-advanced-persistent-threat-malware.html
[10] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Proc. 6th Int. Conf. Inf. Warf. Sec.*, Jan. 2011, pp. 113–125.
[11] *Lifecycle of an Advanced Persistent Threat*, Counter Threat Unit Res., Dell SecureWorks. GSU, Atlanta, GA, USA.
[12] T. Bass, "Intrusion detection systems and multisensor data fusion," *Commun. ACM*, vol. 43, no. 4, pp. 99–105, Apr. 2000.
[13] Y. Zhang, S. Huang, S. Guo, and J. Zhu, "Multi-sensor data fusion for cyber security situation awareness," in *Proc. 3rd Int. Conf. Environ. Sci. Inf. Appl. Technol.*, Oct. 2011, pp. 1029–1034.
[14] A. Stotz and M. Sudit, "Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking," in *Proc. 10th Int. Conf. Inf. Fusion*, Jul. 2007, pp. 1–8.
[15] G. Tadda, J. J. Salerno, D. Boulware, M. Hinman, and S. Gorton, "Realizing situation awareness within a cyber environment," in *Proc. SPIE*, Orlando, FL, USA, 2006, Art. no. 624204.

[16] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, 1976.
[17] P. Smets and R. Kennes, "The transferable belief model," *Art. Intell.*, vol. 66, no. 2, pp. 191–234, Apr. 1994.
[18] J. M. Beaver, R. A. Kerekes, and J. N. Treadwell, "An information fusion framework for threat assessment," in *Proc. 12th Int. Conf. Inf. Fusion*, Jul. 2009 pp. 1903–1910.
[19] H. Wang, J. Hou, and Z. Gong, "Botnet detection architecture based on heterogeneous multi-sensor information fusion," *J. Netw.*, vol. 6, no. 12, pp. 1655–1661, Dec. 2011.
[20] G. Digioia, C. Foglietta, and S. Panzieri, "An agile model for situation assessment: How to make evidence theory able to change idea about classifications," in *Proc. 15th Int. Conf. Inf. Fusion*, Signapore, 2012, pp. 2118–2125.
[21] K. Tang, M.-T. Zhou, and W.-Y. Wang, "Insider cyber threat situational awareness framwork using dynamic bayesian networks," in *Proc. 4th Int. Conf.Comput. Sci. Edu.*, Nanning, China, 2009, pp. 1146–1150.
[22] F. Smarandache and J. Dezert, "Uniform and partially uniform redistribution rules," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 19, no. 6, pp. 921–937, 2011.
[23] M. C. Florea, A.-L. Jousselme, E. Bosse, and D. Grenier, "Robust combination rules for evidence theory," *Inf. Fusion.*, vol. 10, no. 2, pp. 183–197, Apr. 2009.
[24] E. Lefevre, O. Colot, and P. Vannoorenberghe, "Belief function combination and conflict management," *Inf. Fusion*, vol. 3, no. 2, pp. 149–162, Jun. 2002.
[25] S. Maskell, "A bayesian approach to fusing uncertain, imprecise and conflicting information," *Inf. Fusion*, vol. 9, no. 2, pp. 259–277, Apr. 2008.
[26] P. Smets, "Analyzing the combination of conflicting belief functions," *Inf. Fusion*, vol. 8, no. 4, pp. 387–412, Oct. 2007.
[27] W. Lafayette, W. Lafayette, and G. Ghinita, "Towards mechanisms for detection and prevention of data exfiltration by insiders," in *Proc. 6th ACM Symp. Inf. Comput. Commun. Sec.*, Hong-Kong, Jan. 2011, pp. 10–19.
[28] Y. Liu, C. Corbett, K. Chiang, R. Archibald, B. Mukherjee, and D. Ghosal, "SIDD: A framework for detecting sensitive data exfiltration by an insider attack," *42nd Hawaii Int. Conf. Syst. Sci.*, Jan. 2009, pp. 1–10.
[29] D. Smallwood and A. Vance, "Intrusion analysis with deep packet inspection: Increasing efficiency of packet based investigations," in *Proc. Int. Conf. Cloud Service Comput.*, Dec. 2011, pp. 342–347.
[30] J. Grier, "Detecting data theft using stochastic forensics," *Digit. Invest.*, vol. 8, pp. S71–S77, Aug. 2011.
[31] N. R. Suresh, N. Malhotra, R. Kumar, and B. Thanudas, "An integrated data exfiltration monitoring tool for a large organization with highly confidential data source," in *Proc. 4th Comput. Sci. Electron. Eng. Conf.*, Sep. 2012, pp. 149–153.
[32] T. E. Dube, R. A. Raines, M. R. Grimaila, K. W. Bauer, and S. K. Rogers, "Malware target recognition of unknown threats," *IEEE Syst. J.*, vol. 7, no. 3, pp. 467–477, Sep. 2013.
[33] T. Mustafa, "Malicious data leak prevention and purposeful evasion attacks : An approach to advanced persistent threat (APT) management," in *Proc. Saudi Int. Conf. Electron., Commun. Photon. Conf.*, Fira, Greece, Apr. 2013, pp. 1–5.
[34] P. Bhatt and E. T. Yano, "Towards a framework to detect multi-stage advanced persistent threats attacks," in *Proc. IEEE 8th Int. Symp. Service Oriented Syst. Eng.*, Apr. 2014, pp. 390–395.
[35] P. Giura and W. Wang, "A context-based detection framework for advanced persistent threats," in *Proc. Int. Conf. Cyber Secur.*, Washington, DC, USA, Dec. 2012, pp. 69–74.
[36] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Factors: J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 32–64, Mar. 1995.
[37] A. N. Steinberg, C. L. Bowman, and F. White, "Revisions to the JDL data fusion model," *Proc. SPIE*, vol. 3719, pp. 430–441, 1999.
[38] S. Jajodia, S. Noel, P. Kalapa, M. Albanese, and J. Williams, "Cauldron mission-centric cyber situational awareness with defense in depth," in *Proc. MILCOM Milim. Commun. Conf.*, Baltimore, MD, USA, Nov. 2011, pp. 1339–1344.
[39] P. Liu *et al.*, "Cross-layer damage assessment for cyber situational awareness," in *Cyber Situational Awareness. Advances in Information Security*, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA, USA: Springer, 2010, pp. 155–176.
[40] J. Li, X. Ou, and R. Rajagopalan, "Uncertainty and Risk Management in Cyber Situational Awareness," in *Cyber Situational Awareness. Advances in Information Security*, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA, USA: Springer, 2010, pp. 51–68.
[41] P. Harmer, R. Thomas, B. Christel, R. Martin, and C. Watson, "Wireless security situation awareness with attack identification decision support," in *Proc. IEEE Symp. Comput. Intell. Cyber Secur. (CICS)*, Paris, France, Apr. 2011, pp. 144–151.
[42] J. Preden, L. Motus, M. Meriste, and A. Riid, "Situation awareness for networked systems," in *Proc. IEEE Int. Multi-Discipl. Conf. Cognit. Methods Situation Awareness Decision Support (CogSIMA)*, Miami Beach, FL, USA, Feb. 2011, pp. 123–130.
[43] P. Barford *et al.*, "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situational Awareness. Advances in Information Security*, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA, USA: Springer, 2010, pp. 3–4.
[44] J. Okolica, J. T. Mcdonald, G. L. Peterson, R. F. Mills, and M. W. Haas, "Developing systems for cyber situational awareness," in *Proc. 2nd Cyberspace Res. Workshop*, Shreveport, LO, USA, 2009, pp. 46–56.
[45] J. Salerno and G. Tadda, *Overview of Cyber Situational Awareness: Issues and Research* (Cyber Situational Awareness. Advances in Information Security). vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA, USA: Springer, 2010, pp. 15–39.
[46] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proc. IEEE*, vol. 85, no. 1, pp. 6–23, Jan. 1997.
[47] P. Varshney, "Multisensor data fusion," *Electron. Commun. Eng. J.*, vol. 9, no. 6, pp. 245–253, Jan. 1998.
[48] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Ann. Math. Stat.*, vol. 38, no. 2, pp. 325–339, Apr. 1967.
[49] L. A. Zadeh, "Review of a mathematical theory of evidence," *AI Mag.*, vol. 5, no. 3, pp. 81–83, Fall 1984.
[50] R. R. Yager, "On the dempster-shafer framework and new combination rules," *Inf. Sci.*, vol. 41, no. 2, pp. 93–137, Mar. 1987.
[51] D. Dubois and H. Prade, "On the combination of evidence in various mathematical frameworks," in *Reliability Data Collection and Analysis* (Eurocourses: Reliability and Risk Analysis), vol. 3, J. Flamm and T. Luisi, Eds. Dordrecht, The Netherlands: Springer, 1992, pp. 213–241.
[52] P. Louvieris, N. Clewley, and X. Liu, "Effects-based feature identification for network intrusion detection," *Neurocomputing*, vol. 121, pp. 265–273, Dec. 2013.
[53] S. Russel and P. Norvig, "Decision-theoretic agent design," in *Artificial Intelligence a Modern Approach*, 1st ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1995, pp. 508–510.
[54] B. Schneier. (Dec. 1999). *Schneier on Security: Attack Trees*. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html
[55] G. P. Spathoulas and S. K. Katsikas, "Reducing false positives in intrusion detection systems," *Comput. & Secur.*, vol. 29, no. 1, pp. 35–44, Feb. 2010.
[56] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modelling for information security and survivability." Tech. Rep. CMUSEI2001TN001, Mar. 2001.
[57] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
[58] L. Waltz and J. Llinas, *Multisensor Data Fusion*. Norwood, MA, USA: Artech House, 2010.
[59] W. H. Kruskal and W. A. Wallis, "Use of ranks in one-criterion variance analysis," *J. Amer. Stat. Assoc.*, vol. 47, no. 260, pp. 583–621, 1952.
[60] P. Nemenyi, "Distribution-free multiple comparisons," Ph.D. dissertation, Princeton Univ., NJ, USA, 1963.
[61] N. Blenn, V. Ghiëtte, and C. Doerr, "Quantifying the spectrum of denial-of-service attacks through Internet backscatter," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, pp. 21:1–21:10.
[62] *Worldwide Infrastructure Security Report*, Westford, MA, USA, ARBOR Netw., 2016, vol. 10, p. 44.
[63] B. Korby, L. Pièrre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Comput. Sci. Rev.*, vols. 13–14, pp. 1–38, Nov. 2014.
[64] J. Navarro, A. Deruyver, and P. Parrend, "A systematic survey on multi-step attack detection," *Comput. & Secur.*, vol. 76, pp. 214–249, Jul. 2018.
[65] K. E. Heckman, M. J. Walsh, F. J. Stech, A. T. O'Boyle, S. R. DiCato, and A. F. Herber, "Active cyber defense with denial and deception: A cyber-wargame experiment," *Comput. & Secur.*, vol. 37, pp. 72–77, Sep. 2013.

[66] P. Smets, "Belief functions: The disjunctive rule of combination and the generalized Bayesian theorem," *Int. J. Approx. Reas.*, vol. 9, no. 1, pp. 1–35, Aug. 1993.
[67] D. Shen, G. Chen, J. B. Cruz, L. Haynes, M. Kruger, and E. Blasch, "A markov game theoretic data fusion approach for cyber situational awareness," in *Proc. SPIE's Defense Secur. Symp.*, Apr. 2007, pp. 9–13.
[68] K. Tang, M.-T. Zhou, W.-Y. Wang, "Insider cyber threat situational awareness framwork using dynamic Bayesian networks," in *Proc. 4th Int. Conf. Comput. Sci. & Edu.*, Jul. 2009, pp. 1146–1150.
[69] S. J. Yang, S. Byers, J. Holsopple, B. Argauer, and D. Fava, "Intrusion activity projection for cyber situational awareness," in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, Taipei, Taiwan, Jun. 2008, pp. 167–172.
[70] L. Snidaro, I. Visentini, and K. Bryan, "Fusing uncertain knowledge and evidence for maritime situational awareness via markov logic networks," *Inf. Fusion*, vol. 21, no. 1, pp. 159–172, Jan. 2015.

GEORGIOS IOANNOU received the B.Sc. degree in computer engineering from the Alexander Technological Educational Institute, Thessaloniki, Greece, in 2005, the M.Sc. degree in wireless communication systems from Brunel University London, U.K., in 2011, and the Ph.D. degree in computer science from Brunel University London, in 2016.

From 2007 to 2011, he was a Network Engineer with the Greek School Network. He was an IT Engineer with the International Hellenic University, from 2015 to 2017, and was also employed as an Information Security Officer with Interlife Insurance, Thessaloniki, from 2017 to 2018. Since 2018, he has been a Research Fellow with the Digital Economy and Cyber Security Research Group, Brunel University. His research interests are cyber security, cyber situational awareness, information fusion, and the use of distributed ledger technology for e-government.

PANOS LOUVIERIS received the Ph.D. degree in computational continuum mechanics and finite element analysis from The University of Manchester, U.K., in 1983.

He is currently a Professor of information systems with the Department of Computer Science, the Research Director of the Big Data Analytics Cluster, and leads the Digital Economy and Cyber Security Research Group, Brunel University London. He is the Co-Director of the Trusted Open Models Institute, Hartree Centre, U.K., which is a national facility for the development, testing, and classification of the computational models in relation to the use of artificial intelligence. His research interests are in data and information fusion, artificial general intelligence, cyber security, and distributed ledgers for government policy.

Prof. Louvieris was a recipient of the 9th International Command and Control Research and Technology Symposium Best Paper Award, in 2004.

NATALIE CLEWLEY received the B.Sc. degree in information systems, and the Ph.D. degree in information systems research from Brunel University London, U.K., in 2007 and 2011, respectively.

She was a Research Fellow with the Defence and Cyber Security Research Group, Department of Computer Science, Brunel University London, focusing on the use of machine learning and information fusion for Cyber situational awareness and decision support in Cyber Security. The work reported in this paper was undertaken during her employment at Brunel University London. Since 2017, she has been a Lecturer in the human aspects of cyber with the Centre for Electronic Warfare, Information and Cyber, Cranfield University, and is currently based at the Defence Academy of the UK. Her research interests include the use of machine learning, artificial intelligence, and information fusion to support and understand decision making in defense and cyber security.