A Markov Multi-Phase Transferable Belief Model: An Application for predicting Data Exfiltration APTs

Georgios Ioannou
Brunel University
Uxbridge, UK
georgios.ioannou@brunel.ac.uk

Panos Louvieris
Brunel University
Uxbridge, UK
panos.louvieris@brunel.ac.uk

Natalie Clewley
Brunel University
Uxbridge, UK
natalie.clewley@brunel.ac.uk

Gavin Powell
Innovation Works, EADS UK
Newport, UK
gavin.powell@eads.com

***Abstract*— eXfiltration Advanced Persistent Threats (XAPTs) increasingly account for incidents concerned with intelligence information gathering by malicious adversaries. This research exploits the multi-phase nature of an XAPT, mapping its phases into a cyber attack kill chain. A novel Markov Multi-Phase Transferable Belief Model (MM-TBM) is proposed and demonstrated for fusing incoming evidence from a variety of sources which takes into account conflicting information. The MM-TBM algorithm predicts a cyber attacker's actions against a computer network and provides a visual representation of their footsteps.**

Keywords—Cyber Security; Exfiltration; APT; TBM; Information Fusion; Conflict Management

I. INTRODUCTION

Data fusion techniques have found vast acceptance in the field of cyber defence, in the wake of more sophisticated, complex and multi-staged attack vectors. It is considered a powerful capability that can provide significant advances in cyber security [1]. Valuable data may originate from various levels of abstraction, making effective and fast fusion fundamental for enhancing the value of data analysis performed by the deployed security countermeasures, such as intrusion detection systems, firewalls and antivirus software [2]. There is an urgent requirement to detect XAPTs as this category of cyber attacks are used to gather intelligence information by adversaries who seek to gain an advantage through its exploitation.

In previous years, the emergence of Advanced Persistent Threats (APT) has stressed the necessity for incorporating modern techniques to adhere to their multi-staged and multi-target nature. APTs cannot be identified by using common software signatures [3] such as the ones used by commercial intrusion detection systems. The cyber attackers behind those threat vectors "are skilled and well-resourced criminals who employ a wide range of sophisticated reconnaissance and information-gathering tools" [4]. Moreover, APTs can be launched from groups of hackers, either criminal or state-funded and systematically compromise computer networks for years, remaining unidentified from the target's security infrastructure [5]. Some of the most lethal incidents of APTs identified were launched as part of a data exfiltration campaign. These threat models are called XAPTs (eXfiltration APTs). To name a few, operation Aurora [6] targeted 34 large organizations as a medium for industrial espionage. A political figure in Hong-Kong has undergone an XAPT campaign which resulted in a large-scale exfiltration of sensitive data [7]. Operation "Night Dragon" [8] was launched against global oil, energy and petrochemical companies and is another example of industrial espionage.

XAPTs are characterized by systematic and persistent nature of the cyber attackers' actions. An infiltrator will pass through each of the security perimeters with a staged-approach, establish persistence as well as a communications channel between the target and the infiltrator's location, exfiltrate the required information and ultimately erase tracks that could allow forensic investigators to trace their location or even lead to attribution. Those steps produce an equivalent amount of "footprints" which are difficult to monitor and interpret since the frame of discernment becomes very large and spans the individual stages of the threat vector. In addition, cyber attackers use obscurity measures to prevent detection, either through encrypting attack traffic or by masquerading malware as legitimate applications, i.e. trojans. This obscurity can become a source of conflict among the sources of evidence, resulting in counter-intuitive feedback towards the computer network operators, precipitating uncertainty and compromising their cyber situational awareness (SA) [9].

Data fusion techniques are mandatory for addressing the problem of XAPTs since they provide the capability to combine data from heterogeneous sources of evidence and place them within a temporal and spatial framework. Moreover, the incorporation of a conflict management mechanism will enhance the accuracy of the fusion process, eliminate inconsistencies in results and provide the computer network operator with a robust cyber defence capability [10].

The purpose of this paper is to propose a novel data fusion algorithm that will effectively fuse incoming and potentially conflicting evidence from sources of evidence within the network, in order to mitigate XAPTs. In addition, the algorithm will provide the capability to predict future activities on behalf of the attacker during an attack campaign. Section II presents the underlying theories for conflict management and attack kill chains, Section III describes the proposed model and Section IV presents the operation of the model using example data. Section V provides a discussion on the model and the assumptions that will be addressed in future research.

This work is sponsored by DSTL (Cyber & Influence Science & Technology Centre) and EADS Innovation Works

II. THEORETICAL DEVELOPMENT

A. Evidence Theories and the issue of conflict management

Dempster-Shafer theory (DST) [11] which is also known as the theory of evidence is a means for representing epistemic uncertainty. The Transferable Belief Model (TBM) [12], is an alternative interpretation of DST, differentiated in respect of the open/closed world assumption. In both, the basis for describing the knowledge of the state of the "world" is defined from the frame of discernment $\Omega = \{\omega_1, \omega_2, \dots \omega_n\}$. Ω is a set of all the possible states of the described 'world'. In a closed world (DST), the elements of the frame are mutually exclusive and exhaustive, whereas in an open world (TBM), exhaustive frames are not a requirement. The power set 2^{Ω} contains all the possible subsets of Ω. A basic belief assignment (bba) or basic belief mass (bbm) is a mapping m from $2^{\Omega} \rightarrow [0, 1]$ for $\sum_{A \subseteq \Omega} m(A) = 1$.

DST perceives ignorance as a lack of knowledge which implies that all known hypotheses are equally likely (expressed as $m(\Omega) = 1$); on the other hand, TBM considers ignorance as an indication of problematic hypotheses assessment or as incredibility on behalf of the sources of evidence [13]; this is expressed by a mass assignment upon the null set (Ø). This differentiation is reflected upon the combination rule that is implemented in each of the two theories; DST employs a normalization factor that evenly redistributes the concentrated conflict to the remaining hypotheses, whereas TBM does not. Given B, C and X subsets of Ω, Dempster's combination rule is given in (1) and Smets' combination rule (or conjunctive rule) is given in (2).

$$m(X) = \sum_{B,C \subseteq \Omega; B \cap C = X} \frac{m(B)m(C)}{1-k}, k = \sum_{B \cap C = \emptyset} m(B)m(C) \quad (1)$$

$$m(X) = \sum_{B \cap C = X} m(B)m(C) \quad (2)$$

Zadeh [14] identified the problematic behaviour of Dempster's combination rule [11] upon situations where the conflict among the sources of evidence is very high. Smets has proposed the conjunctive combination rule [13] as a replacement and allowed for the observed conflict to be reflected as a belief mass assignment upon the null set m(Ø). This property has caused criticism [15][16], based on the fact that m(Ø) can become intractable even for a relatively small number of sources (less than 4) and a limited number of hypotheses (less than 4). The presence of high conflicting mass is considered counter intuitive; furthermore, even if newer sources are not contributing to conflict (they are in full agreement with previous sources), the conflict mass cannot be reduced.

Smets defends his approach [13] by claiming that a high conflict is an indicator of a malfunctioning expert system and should be exploited as an alert event. Nevertheless, the pignistic transformation of TBM which converts belief masses to probabilities employs a normalization factor identical to that of Dempster's combination rule and hence eliminates conflict as well. Equation (3) illustrates the pignistic transformation.

$$BetP(A) = \sum_{B \subseteq \Omega} \frac{|A \cap B|}{|B|} \frac{m(B)}{1 - m(\emptyset)}, \forall A \in \Omega \quad (3)$$

Indeed, the presence of conflict is an indication of "disagreement" among the sources of evidence. In practice conflict mass is generated when fully contradicting beliefs are combined using Smets' conjunctive combination rule. Additional combination rules have been proposed, such as the family of Partial Conflict Redistribution (PCR) rules [17] and the Robust Combination Rules (RCR) [18]. Those solutions provide more intuitive results compared to the conjunctive rule as belief masses will always be assigned on some of the known hypotheses. However, for the purposes of this paper, the amount of generated conflict is not considered a drawback; influenced by Smets' perception of m(Ø), the presented approach considers conflict mass manageable. Conflict management is achieved by decomposing the underlying problem (such as XAPTs) into multiple stages which are described by multiple frames.

The belief assignments that are reported by the sources and correspond to each phase will be fused using Smets' combination rule. Any conflict mass generated due to the combination will be reset at each transition between the phases. Further justification on the conflict resetting is given below.

B. Attack kill chains

XAPTs do not produce a common signature that can be incorporated within an intrusion detection/prevention system and be detected accordingly. Nevertheless, what is common among XAPT variants is that a sequence of actions is required on behalf of the attacking group in order to reach its ultimate goal. It is almost certain that this sequence of activities will occur in any XAPT attempt. Kill chain models that describe phases of intrusions are given in [5][19]. In [5], the authors combine knowledge obtained from previous attacks observed in various cases and form a kill chain as a paradigm for modelling XAPTs. Hutchins et al. [19] exploit the evidence obtained by attacks suffered within their organization and stress how the kill chain approach enables early detection and mitigation of XAPTs.

Although there exist different interpretations of the evidence that are observed ([5] and [19]) during the course of an XAPT, it is evident that a common framework exists within every attacking group's plan. Their plan ensures that their attack will proceed systematically; the actions that are taking place at each phase of the XAPT are directly affected by the outputs of the preceding one. The *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 *Command & Control (C2)* phase involves the control traffic from the attacker's location and the collateral 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 C2 phase.

C. A Markov process kill chain for modelling XAPTs

A Markov process is a stochastic modelling technique which is based on the Markov property of systems behaviour [20]. The future state X_{n+1} of a discrete time Markov process in time $n+1$ is dependent only upon the current state X_n and not on any of the previous states ($1,2,\ldots, n-2, n-1$). Transitioning between each state can be associated with a probability mass.

The kill chain model assessed in this paper satisfies the Markov property; the next action of an attacker and its impact on the target network can be modelled using a probability measure. This measure is called a *prior belief*. This value defines the belief of the system upon the attacker's next action, during the course of an XAPT campaign. Table I illustrates the kill chain model adopted in this paper.

The attackers' actions are determined by the properties of the target network, such as software vulnerabilities, security policies and countermeasures, network architecture, operating systems, running services and the location of the valuable data to be exfiltrated. This work exploits the multiphase (sequence) nature of an XAPT attack into its constituent components and maps it into a kill chain. An XAPT will commonly aim at exfiltrating data from a High-Valued Target (HVT), i.e. a database server containing classified information. Since the ultimate target of a potential attack can be determined beforehand and given the network layout, a security assessment can reveal the pathways that attackers may follow to reach their goal. A tree-structure can successfully model and provide a visual representation of the phases that an XAPT can progress and enable prediction of its future states.

By combining the obtained knowledge from the sources of evidence, the prior beliefs and the tree-structure, the estimation of a predicted belief upon the attackers' ultimate goal can be calculated ($m_{predicted}$). Each level of the tree corresponds to a phase of an XAPT; the nodes that co-exist within a tree level are mapped to the corresponding attack vectors that can be utilised within a phase.

TABLE I. KILL CHAIN

Phases	Description
Reconnaissance	TCP Port scanning, service probing, social engineering tactics.
Insertion	Spear-phishing, brute-force/dictionary attacks.
Exploitation	Launch exploits against software vulnerabilities, SQL injection, remotely install malware (backdoor/trojan/rootkit).
Command & Control (C2)	Privilege escalation, pivoting, file-system and database browsing, additional malware installation.
Exfiltration	Upload data using encrypted covert channels to external storage media or a cloud.

This divide-and-rule approach of addressing the problem of XAPTs allows for conflict reset between each phase of the kill chain. As the system transitions to a next phase by tracking malicious behaviour, the previously obtained knowledge from evidence sources can be considered as obsolete. The system focuses upon new sources, determined by the children of the current node, hence the uncertainty generated and allocated within m(Ø) can be considered obsolete as well.

The proposed algorithm implements a tree structure that will be based on a scenario of an office network that includes a High-Valued Target (HVT). The expansion of this model to a large-scale network with multiple HVTs and a more complex infrastructure is considered trivial, since its design can be directly influenced by a cyber security assessment which is a requirement for maintaining a high-level of security within an organisation's network. The sources of evidence are dependent upon the application and are not discussed in this paper. The proposed model assumes the presence of several sources that operate within the security context and produce their outputs as belief assignments.

Moreover, the proposed model incorporates strategic lock-out of hypotheses, by pruning the branches of the tree that have not been assigned any support by the fused belief masses. This technique enables the network operators to:

1. Limit the hypothesis space and to focus on specific sources of evidence.
2. Reduce the number of computations for predicting future attacker's actions by assessing a smaller number of hypotheses and hence reducing their response time.
3. Efficiently plan their mitigation strategy.

A detailed description of the Markov Multi-Phase TBM (MM-TBM) is given in the next section.

III. MARKOV MULTI-PHASE TBM

The basic elements of the MM-TBM model are described below in terms of *Knowledge Management-tree pruning* and *Belief Propagation*.

A. Knowledge Management – tree pruning

XAPTs are composed of a series of attack steps that occur in a phased approach. A number of specialized malware is utilized during an XAPT, commonly associated with each phase. Conventional intrusion detection systems are signature-based because they employ pattern matching and classification techniques and the observed evidence is associated with known attack signatures. Maintaining signatures for multi-staged attacks that may follow various paths is a complex process.

In our proposed model, the potential attackers' behaviour is modelled using a tree structure which is represented as the set $T = \{N, B, P\}$, where:

- N is a subset that contains the nodes N_{ij} of the tree T, with i being the index of the tree-level (and the phase of the kill chain) and j the index of the node within tree-level i.

- B is a subset that contains the directed branches $B_{ijmn}(N_{ij}, N_{mn})$ that connect nodes N_{ij}, and N_{mn} with $m = i+1$ since N_{mn} is in the next phase of N_{ij}.
- P is a subset that contains the prior beliefs $P(B_{ijmn})$ for the branches of B.

$S(T, N)$ is defined as a sub-tree of T with N being the root node.

MM-TBM incorporates two levels of knowledge for facilitating the monitoring of current malicious activities and enabling prediction for future actions. The two levels of knowledge are represented by the Alert and the Awareness frames of discernment. Whenever an attack is detected, its matching node upon the tree is activated. This event triggers the initialisation/update of the two frames:

- The *Alert frame* (Ω_{al}) contains the next actions that an attacker may follow, based on the previously observed evidence. Ω_{alp} is defined as the Alert frame that has been initialized for phase p, based on the received evidence. These actions will always belong to a specific phase of the kill chain.

$$\Omega_{alp} = \{N_{p1}, N_{p2}, \dots N_{pj}\} \text{ with } j = |\Omega_{alp}| \quad (4)$$

  The Alert frame is constructed by the children nodes of the last activated nodes from the current phase N_{ij}, with $i = p-1$ (but not their descendants). Whenever a new Alert frame is created, the sources of evidence are focusing on those specific resources of the network that can provide feedback related to the elements of the frame. The children of nodes that have not been assigned a belief are marked for deletion. If none of the children of a node that was a member of the Alert frame in the previous phase receives any amount of belief, then this node (as well as the sub-tree below it) is pruned from the tree as well. The belief that was assigned to this node in the previous phase is evenly distributed among its activated siblings.

- The *Awareness frame* (Ω_{aw}) contains all the paths of the tree that reach to a terminal node, omitting those paths that begin from a node which has not been allocated a belief. The frame is derived by performing a depth-first search on the tree, starting from the root node of the tree and leaving out the sub-trees which have a root node N_{del} that has been marked for deletion. The new tree is given by:

$$T' = T - S(N_{del}, T) \quad (5)$$

  The terminal nodes refer to the *Exfiltration* phase; this frame informs the network operator on the attackers' potential future actions until they reach their ultimate goal. The omitted paths are pruned and the tree is reshaped, containing only the active paths.

The branches of the tree are labelled with a matching prior belief. The sum of prior beliefs of the directed branches that originate from a node will always be equal to 1. The value of the prior belief indicates the model's belief as regards the next step of the attacker.

B. Belief Propagation

Belief propagation is employed for estimating the future actions of the attackers, based on the obtained knowledge from the sources of evidence and the prior beliefs that are assigned to the tree branches. The process is as follows:

1. Combine the received evidence using the conjunctive rule in (2).
2. Calculate the pignistic probability for each of the nodes of the Alert frame for phase p, by applying the pignistic transformation upon the fused beliefs. Set the conflict mass that was generated by the application of the conjunctive rule for phase p to 0: $m_p(\emptyset) \leftarrow 0$. The pignistic transformation is given in (6).

$$BetP(N_{pi}) = \sum_{X \subseteq \Omega_{alp}} \frac{|X \cap N_{pi}|}{|X|} \frac{m(X)}{1 - m_p(\emptyset)}, \forall N_{pi} \in \Omega_{alp} \quad (6)$$

   Where Ω_{alp} is the alert frame of phase p, N_{pi} is any given node of Ω_{alp} for which the pignistic probability must be calculated, X is a subset of Ω_{alp} and $m_p(\emptyset)$ the generated conflict at phase p.
3. Overwrite the priors for the branches that lead to these nodes with the pignistic values.
4. Calculate the joint belief for each path, starting from the root node of the tree.

The output will contain a number of predicted beliefs ($m_{predicted}$), one for each of the elements of the Awareness frame. The joint belief for each path is given by the following formula:

$$m_{predicted}(path) = \prod_{A_i \in path} m(A_i) \quad (7)$$

An illustration of the algorithm is given in Fig. 1.

IV. An Example Application Of MM-TBM

The presented example illustrates how MM-TBM tracks the phases of an XAPT when launched against a small network that contains one HVT. The purpose of this example is to demonstrate how the fused beliefs from the sources of evidence are reflected in the tree structure, the way that hypotheses are eliminated using tree pruning and the belief propagation for making predictions upon the hypotheses contained in the Awareness frame.

Table II illustrates the individual events that are described by the kill chain and their abbreviations. The tree for the given scenario is illustrated in Fig. 2. Each node is labelled with its matching abbreviation and a prior belief. Two remarks must be made at this stage:

1. The branches that originate from nodes that have only one child are automatically assigned a prior belief of 1. This assumption is made on the basis that, when only one child exists, this child node represents the only potential outcome.

2. Some nodes are repeated in more than one branch. This phenomenon does not affect the validity of the model; instead, it offers a more convenient visual representation for the network operator.

Table III illustrates the beliefs that are received by the sources of evidence at phase 1, the fused beliefs derived by applying the conjunctive rule and the pignistic values calculated by the pignistic transformation.

In this simple case of a tree with only one root node, all the elements of Ω_{aw} are assessed, since both the children nodes of the root node are marked as active. The corresponding tree for phase 1 as well as for the rest of the phases is given in the Appendix.

Table III illustrates the conversion of the received belief to a pignistic probability, the alert and awareness frames based on the incoming evidence and the predicted beliefs that are calculated by applying belief propagation. The values of the predicted beliefs are reflecting the model's belief on the attacker's future activities. Table IV illustrates the same process as soon as the next evidence has been received.

A belief assignment is assigned only to the *SMB*, hence *SP* and its sub-tree are pruned. The associated hypotheses from Ω_{aw} are removed and a new awareness frame is constructed. The new Ω_{al} informs the sources of evidence on the new hypotheses. Tables V, VI and VII illustrate the following phases. At the first phases of the attack, the number of hypotheses contained in the Ω_{aw} (equal to 10) and the corresponding predicted beliefs are hard to monitor and evaluate.

However, as the attack progresses MM-TBM limits the hypothesis space and dedicates an amount of belief to each of the possible scenarios. This permits the network operators to assess their mitigation strategy at an early stage of the attack campaign. When the last piece of evidence is received, the last phase has been assessed and the leaf nodes of the tree have been reached, hence there is no requirement for obtaining a new Alert frame.

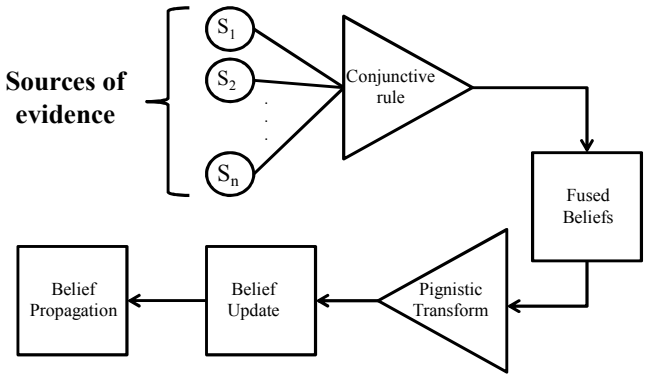

Fig. 1. Belief Update and Propagation

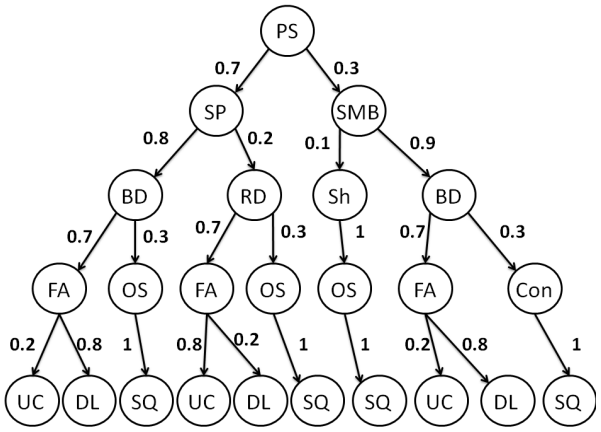

Fig. 2. Tree at phase 0

Based on the evidence, the hypothesis (PS, SMB, BD, FA, DL) is output as the most likely, assigned a belief value of 0.96, compared to the belief value of the competing hypothesis, (PS, SMB, BD, FA, UC) which is equal to 0.04.

V. DISCUSSION

A valuable amount of information can be collected about the opposition's skills and methods by monitoring their behaviour and attack strategies.

TABLE II. EVENTS OF THE KILL CHAIN

Phase	Event	Abbreviation
Reconnaissance	Port Scan	PS
Insertion	Spear Phishing	SP
	SMB Exploit	SMB
Exploitation	Backdoor	BD
	Remote Desktop	RD
	Shell	Sh
Command & Control	File Access	FA
	Osql2DB	OS
	Connect to DB	Con
Exfiltration	Upload to Cloud	UC
	Download locally	DL

TABLE III. PHASE 1

Phase 1: Reconnaissance		
Received beliefs	***Fused beliefs (conjunctive rule)***	***BetP***
m(PS) = 1	m(PS) = 1	BetP(PS) = 1
Alert frame	***Awareness frame***	
{PS, SP}	{(PS, SP, BD, FA, UC), (PS, SP, BD, FA, DL), (PS, SP, BD, OS, SQ), (PS, SP, RD, FA, UC), (PS, SP, RD, FA, DL), (PS, SP, RD, OS, SQ), (PS, SMB, Sh, OS, SQ), (PS, SMB, BD, FA, UC), (PS, SMB, BD, FA, DL), (PS, SMB, BD, Con, SQ)}	
Predicted Beliefs		
m_p (PS, SP, BD, FA, UC) = 0.0784 m_p (PS, SP, BD, FA, DL) = 0.3136 m_p (PS, SP, BD, OS, SQ) = 0.168 m_p (PS, SP, RD, FA, UC) = 0.0784 m_p (PS, SP, RD, FA, DL) = 0.0196 m_p (PS, SP, RD, OS, SQ) = 0.042 m_p (PS, SMB, Sh, OS, SQ) = 0.03 m_p (PS, SMB, BD, FA, UC) = 0.0378 m_p (PS, SMB, BD, FA, DL) = 0.1512 m_p (PS, SMB, BD, Con, SQ) = 0.081		

MM-TBM offers the capability for monitoring attackers' activity as they transit through the phases of the kill chain. The responses of a cyber network operator in the wake of an incoming attack vary.

TABLE IV. PHASE 2

Phase 2: Insertion		
Received beliefs	***Fused beliefs (conjunctive rule)***	***BetP***
m_1 (SMB) = 0.7 m_1 (Ω_{al}) = 0.3 m_2 (SMB) = 1	m_{12} (SMB) = 1	BetP(SMB) = 1
Alert frame	***Awareness frame***	
{Sh, BD}	{(PS, SMB, Sh, OS, SQ), (PS, SMB, BD, FA, UC), (PS, SMB, BD, FA, DL), (PS, SMB, BD, Con, SQ)}	
Predicted Beliefs		
m_p (PS, SMB, Sh, OS, SQ) = 0.1 m_p (PS, SMB, BD, FA, UC) = 0.126 m_p (PS, SMB, BD, FA, DL) = 0.504 m_p (PS, SMB, BD, Con, SQ) = 0.27		

TABLE V. PHASE 3

Phase 3: Exploitation		
Received beliefs	***Fused beliefs (conjunctive rule)***	***BetP***
m_1 (Sh) = 0.6 m_1 (Ω_{al}) = 0.4 m_2 (BD) = 0.5 m_2 (Sh) = 0.5	m_{12} (Sh) = 0.5 m_{12} (BD) = 0.2 m_{12} (Ø) = 0.3	BetP(Sh) = 0.625 BetP(BD) = 0.375
Alert frame	***Awareness frame***	
{Con, FA, OS}	{(PS, SMB, Sh, OS, SQ), (PS, SMB, BD, FA, UC), (PS, SMB, BD, FA, DL), (PS, SMB, BD, Con, SQ)}	
Predicted Beliefs		
m_p (PS, SMB, Sh, OS, SQ) = 0.625 m_p (PS, SMB, BD, FA, UC) = 0.0525 m_p (PS, SMB, BD, FA, DL) = 0.21 m_p (PS, SMB, BD, Con, SQ) = 0.1125		

Commonly, the identification of a breach leads to shutting down legitimate services that either have already been compromised or are susceptible to attack. An elevation of the security policy to a higher level of security can be triggered by the detection of an attack. In addition, deception techniques such as honeypots may be employed to "trap" attackers within a "bogus" host and collect further information on their intentions or weaponry. MM-TBM is designed to inform network operators about the current state of the computer network when an XAPT is present and for providing early detection.

TABLE VI. PHASE 4

Phase 4: C2		
Received beliefs	***Fused beliefs (conjunctive rule)***	***BetP***
m_1 (Con) = 0.3 m_1 (FA) = 0.7 m_2 (FA) = 0.7 m_2 (Ω_{al}) = 0.3	m_{12} (FA) = 0.7 m_{12} (Con) = 0.09 m_{12} (Ø) = 0.21	BetP(FA) = 0.89 BetP(Con) = 0.11
Alert frame	***Awareness frame***	
{UC, DL, SQ}	{(PS, SMB, BD, FA, UC), (PS, SMB, BD, FA, DL), (PS, SMB, BD, Con, SQ)}	
Predicted Beliefs		
m_p (PS, SMB, BD, FA, UC) = 0.178 m_p (PS, SMB, BD, FA, DL) = 0.712 m_p (PS, SMB, BD, Con, SQ) = 0.11		

TABLE VII. PHASE 5

Phase 5: Exfiltration		
Received beliefs	***Fused beliefs (conjunctive rule)***	***BetP***
m_1 (DL) = 0.9 m_1 (Ω_{al}) = 0.1 m_2 (DL) = 0.7 m_2 (UC) = 0.3	m_{12} (DL) = 0.7 m_{12} (UC) = 0.03 m_{12} (Ø) = 0.27	BetP(DL) = 0.96 BetP(UC) = 0.04
Alert frame	***Awareness frame***	
-	{(PS, SMB, BD, FA, UC), (PS, SMB, BD, FA, DL)}	
Final Beliefs		
m_p (PS, SMB, BD, FA, UC) = 0.04 m_p (PS, SMB, BD, FA, DL) = 0.96		

The proposed model will enhance network operators' cyber SA, providing a fully updated perception of the underlying environment in a timely manner, by incorporating expert knowledge from the attack kill chains into a data fusion technique that is capable of eliminating conflict from the sources of evidence and provide a visual representation of the environment's status during the progression of an XAPT.

The performance of the proposed algorithm and its prediction accuracy relies on two factors:

1. The prior beliefs. The priors are manually assigned to the tree branches based on a security assessment. The model also offers the capability for tuning the prior beliefs during operation, as a response to new information, such as a zero-day exploit that can be employed to compromise a component of the network. In the awake of a new exploit which has been discovered 'in the wild', sophisticated attackers are likely to attempt to use this exploit against the target network, therefore the network components that are affected by this exploit are more likely to undergo an attack.
2. The assessment of the sources of evidence. A requirement for MM-TBM is the existence of an underlying collection of sources of evidence that will act as the sensors of the proposed fusion algorithm. The selection of the valid sources is dependent on the application; the network infrastructure and installed software may vary. The network components can provide a collection of raw data, such as network packet capture, file-system and registry monitoring tools, intrusion detection systems alerts, or machine learning algorithms such as supervised/unsupervised learning. Most of these sources provide feedback in categorical form (Attack/Normal). Since TBM fusion requires belief functions to operate; further assessment is required for converting the output of those sources to belief assignments. Three methods for combining results from supervised learners are given in [21]. The credibility of each classifier is calculated by measuring the performance of each classifier and is applied as a weight for each classifier, producing values in [0, 1]. Methods for building belief functions on compound hypotheses instead of singletons is given in [22].

The above factors are expected to play an important role in the overall performance of the proposed model. For the purpose of this paper, the above features have not been considered but will be addressed in future research.

VI. CONCLUSIONS AND FURTHER WORK

This paper proposes a novel data fusion algorithm, the MM-TBM, for hypotheses assessment and managing conflict within the sources of evidence from the network. This will enable detection of XAPTs, thus enhancing cyber situational awareness and understanding cyber network operators. This paper has demonstrated that the limitations of the traditional TBM associated with managing conflicting evidence sources are overcome by employing the MM-TBM. The MM-TBM enables the reduction of the Frame of Discernment by employing strategic lock-out based on the incoming evidence. This permits a focus on specific sources of evidence, omitting the ones that are potentially uninformative hence reducing the computational effort. Future research will address the application of the MM-TBM to other domains characterised by multi-phased problems.

REFERENCES

[1] N. A. Giacobe, "Application of the JDL Data Fusion Process Model for Cyber Security," in Proc. SPIE, 2010, p. 77100R..

[2] I. Corona, G. Giacinto, C. Mazzariello, F. Roli, and C. Sansone, "Information fusion for computer security: State of the art and open issues," *Information Fusion*, vol. 10, no. 4, pp. 274–284, Oct. 2009.

[3] G. Thomson, "APTs: a poorly understood challenge," Network Security, vol. 2011, no. 11, pp. 9–11, Nov. 2011.

[4] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, Aug. 2011.

[5] MANDIANT, "M-Trends: The Advanced Persistent Threat," Washington, DC, 2010.

[6] B. E. Binde, R. Mcree, and T. J. O. Connor, "Assessing Outbound Traffic to Uncover Advanced Persistent Threat", SANS Technology Institute, 2011.

[7] F. Li, "A Detailed Analysis of an Advanced Persistent Threat Malware.", SANS Technology Institute, 2011.

[8] B. Mcafee, P. Services, and M. Labs, "Global Energy Cyberattacks : 'Night Dragon '", McAfee, 2011.

[9] M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems", *Human Factors*, vol. 37, no. 1, pp. 32–64, Mar. 1995.

[10] S. J. Yang, A. Stotz, J. Holsopple, M. Sudit, and M. Kuhl, "High level information fusion for tracking and projection of multistage cyber attacks," *Information Fusion*, vol. 10, no. 1, pp. 107–121, Jan. 2009.

[11] G. Shafer, A Mathematical Theory of Evidence. Princeton University Press, 1976.

[12] P. Smets and R. Kennes, "The transferable belief model," *Artificial Intelligence*, vol. 66, no. 2, pp. 191–234, April 1994.

[13] P. Smets, "Analyzing the combination of conflicting belief functions," *Information Fusion*, vol. 8, no. 4, pp. 387–412, Oct. 2007.

[14] L. Zadeh, "Reviews of books, a mathematical theory of evidence," *AI Magazine*. v5 i3, vol. 5, no. 3, pp. 81–83, Sept. 1984.

[15] J. Dezert and F. Smarandache, "Advances and applications of DSmT for information fusion," Am. Res. Press, Rehoboth, vol. 1, 2004.

[16] A. Martin, A.-L. Jousselme, "Conflict measure for the discounting operation on belief functions", in *Information Fusion*, *11th International Conference on*, 2008 pp.1-8.

[17] F. Smarandache and J. Dezert, "Extended PCR rules for dynamic frames," in *Information Fusion (FUSION), 2012 , 15th International Conference on*, 2012, pp.263–270.

[18] M. Florea, A. Jousselme, E. Bosse, and D. Grenier, "Robust combination rules for evidence theory," *Information Fusion*, vol. 10, no. 2, pp. 183–197, April 2009.

[19] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *The 6th International Conference on Information-Warfare & Security*, 2011, Academic Conferences Ltd., 2010, pp. 113–125.

[20] A. Pfening and M. Telek, "Optimal control of Markov regenerative processes," in *Systems, Man, and Cybernetics, 1998. 1998 IEEE International Conference on*, 1998, vol. 1, pp. 663–668.

[21] D. Mercier, G. Cron, T. Denoeux, and M. Masson, "Fusion of multi-level decision systems using the transferable belief model," *2005 7th International Conference on Information Fusion*, p. 8, 2005.

[22] D. Veremme, A.Dupont, D. Lefevre and E. Mercier, "Belief assignment on compound hypotheses within the framework of the Transferable Belief Model," *Information Fusion, 2009. FUSION '09. 12th International Conference on*, pp. 498–505, 2009.

APPENDIX

This Appendix contains the trees constructed during each phase of the presented example in Section IV. Fig. 3 illustrates the updating of the priors with pignistic probabilities.

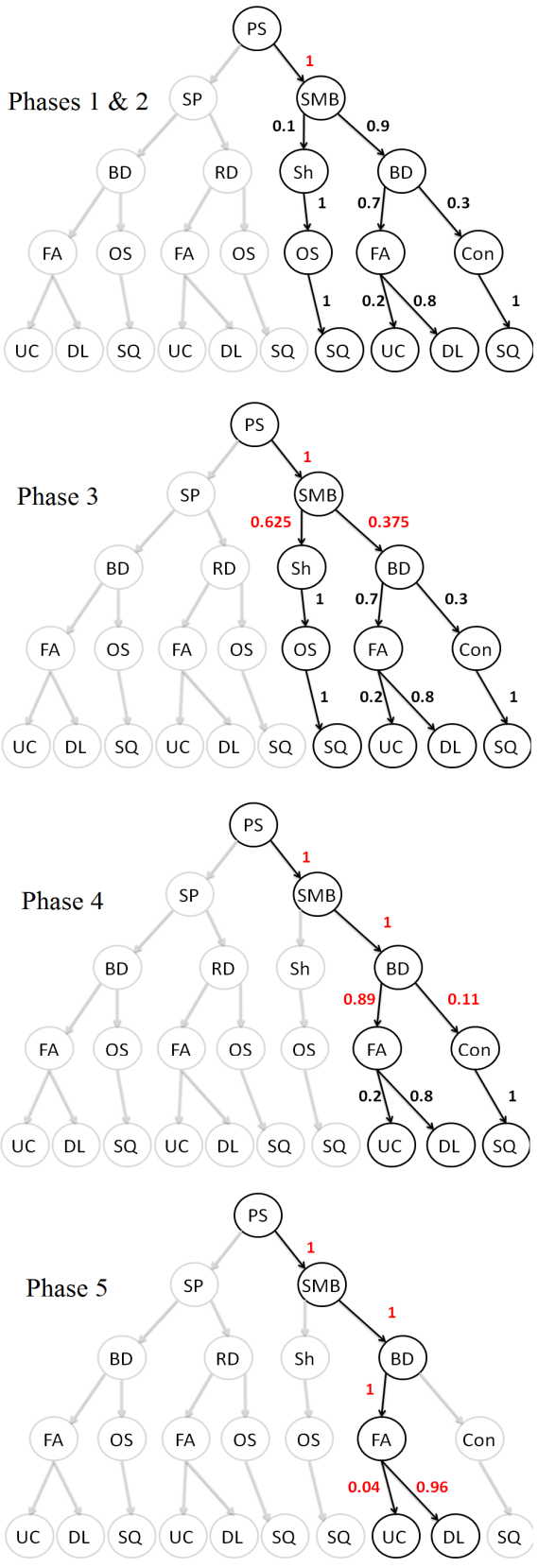

Fig. 3. Updating of priors with pignistic probabilities