Sombrero Dynamic Honeynet Defense

Ken F. Yu, Daniel T. Sullivan, Dr. Edward J. Colbert

1. MOTIVATION

In this work, we explore methods of preserving the mission of a hypothetical military outpost, which we label "Sombrero", in the event that it is impossible to reduce its radio-frequency (RF) emission sufficiently to hide its location. As wireless and RF-emitting devices become more commonplace in military environments, systems will suffer an increasingly difficult problem of hiding from adversaries. This problem will become exponentially more difficult as the commercial IoT (Internet-of-Things) and the corresponding tactical IoBT (Kott et al., 2016) grows in size. The attack surface of future tactical environments will become dangerously complex. Potential cyber vulnerabilities of insecure devices will magnify threats to the physical world of humans (soldiers), and potential physical attacks, including electronic warfare (EW) attacks on RF devices, will allow previously unrealized attack vectors into cyber systems. The impact of a military outpost being radio-loud can have extreme consequences in a battle, and solutions to the problem are warranted. We describe a few methods of camouflaging a radio-loud outpost, and we focus in particular on a solution involving cyber decoys, or "honeynets."

Physical and logical camouflage or decoys can act as active countermeasures to protect radio-loud outposts (see Figure 1). The outpost may be camouflaged by creating one or more physical decoys consisting of near-identical or more interesting artificial RF emissions that seem to be originating from other geographical locations. Similarly, the outpost may be camouflaged from cyber attack by creating one or more logical decoys (honeynets), which appear to be the actual protected cyber network, or a network that is more interesting to potential attackers.

In this work, we focus on cyber camouflage using dynamically created honeynets, although, in practice, one might want to implement various combinations of physical and logical camouflage techniques.

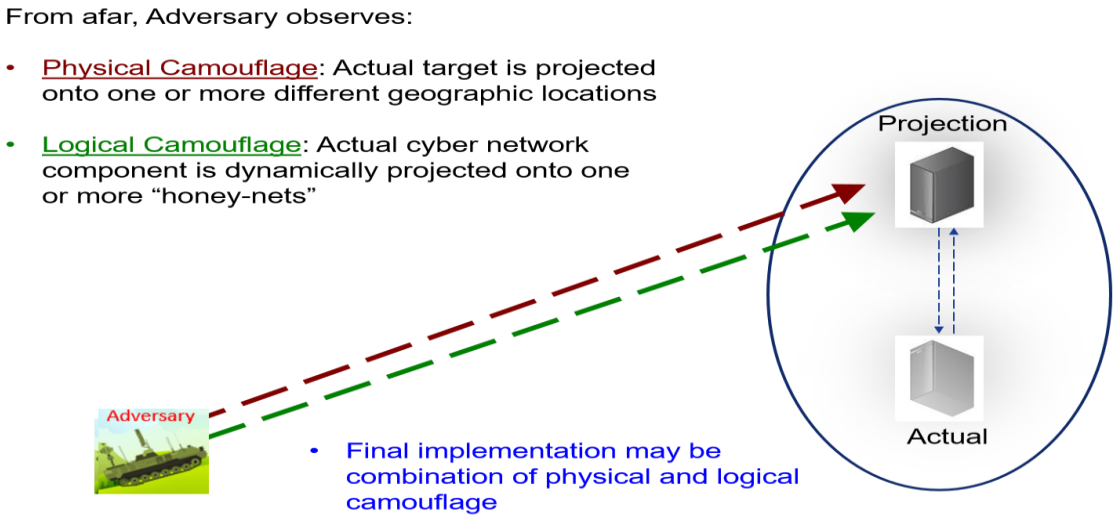

Figure 1 – Adversarial view of physical and logical camouflage techniques using decoys.

For defending of the hypothetical Sombrero outpost and resilience of its mission, we attempt to deceive cyber attackers before or quickly after they launch a cyber attack by standing up a virtual network labyrinth (honeynet) that is both realistic and attractive to the adversary. As the cyber attacker continues further into honeynet, the Sombrero defense system utilizes past knowledge and dynamic, real-time, decision-making algorithms to engage the adversary, thus reducing or eliminating the threat on the actual network.

Figure 2 shows an operational view of the Sombrero dynamic honeynet defense system protecting a military outpost.

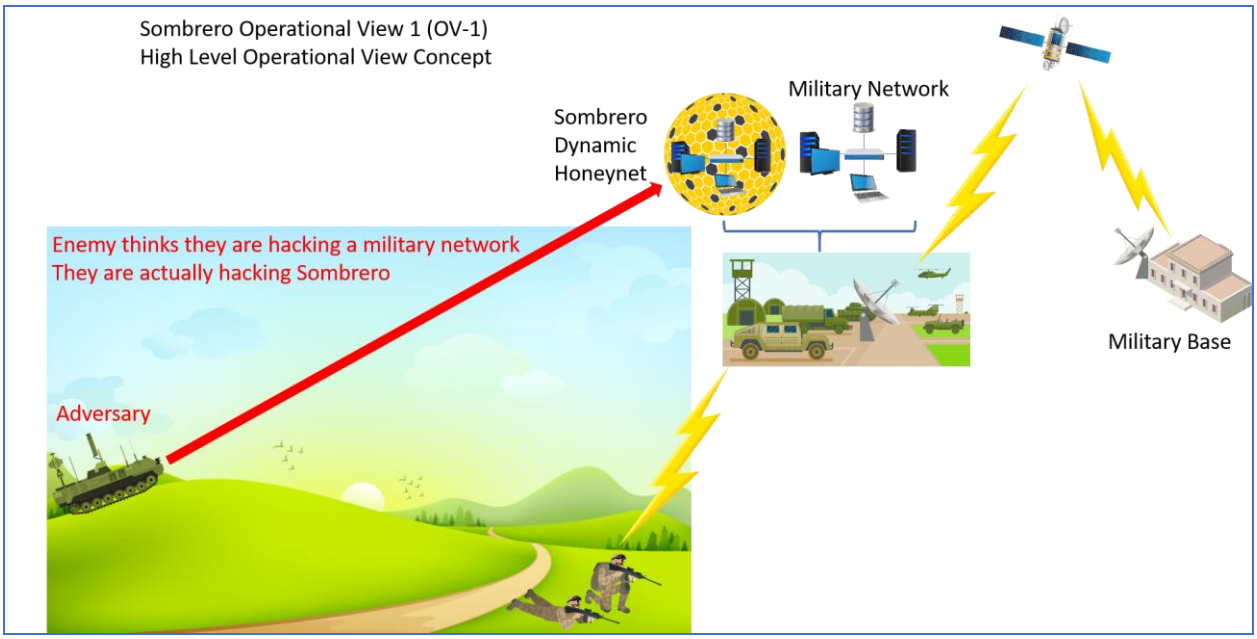

Figure 2 – Sample of Sombrero dynamic honeynet implementation.

Sombrero will depend upon technology from many domains. Physical EM sensor and network sensors will need to detect the cyber adversaries, machine learning (ML) detection algorithms must be intelligent enough to detect spoofing attempts or injection of adversarial sensor data, and cognitive models and game theory (Chung et al., 2016) will be needed to estimate adversarial intent and goals. Sombrero must have high enough fidelity in its simulated or emulated devices to appear realistic to the attacker and autonomously create virtual "bait" for the enemy to pursue.

2. SYSTEM ARCHITECTURE

Sombrero is a highly sophisticated system that has to meet the many challenges all military networks must face in the future. Before building such a complicated system, many critical questions have to be answered and be met. Questions such as, how do we validate which communication is trusted? How do we handle insider threats? How to we build a system that is capable of performing self-learning and self-updating? How do we entice the attacker to pursue the honeynets instead of the real system? How to we interpret INTEL gathered on an attacker and feed it back to Sombrero? To meet these challenges, Sombrero has to meet many critical requirements, such as self-learning and self-updating. In Figure 3, we illustrate the information flow of a conceptual Sombrero system architecture.

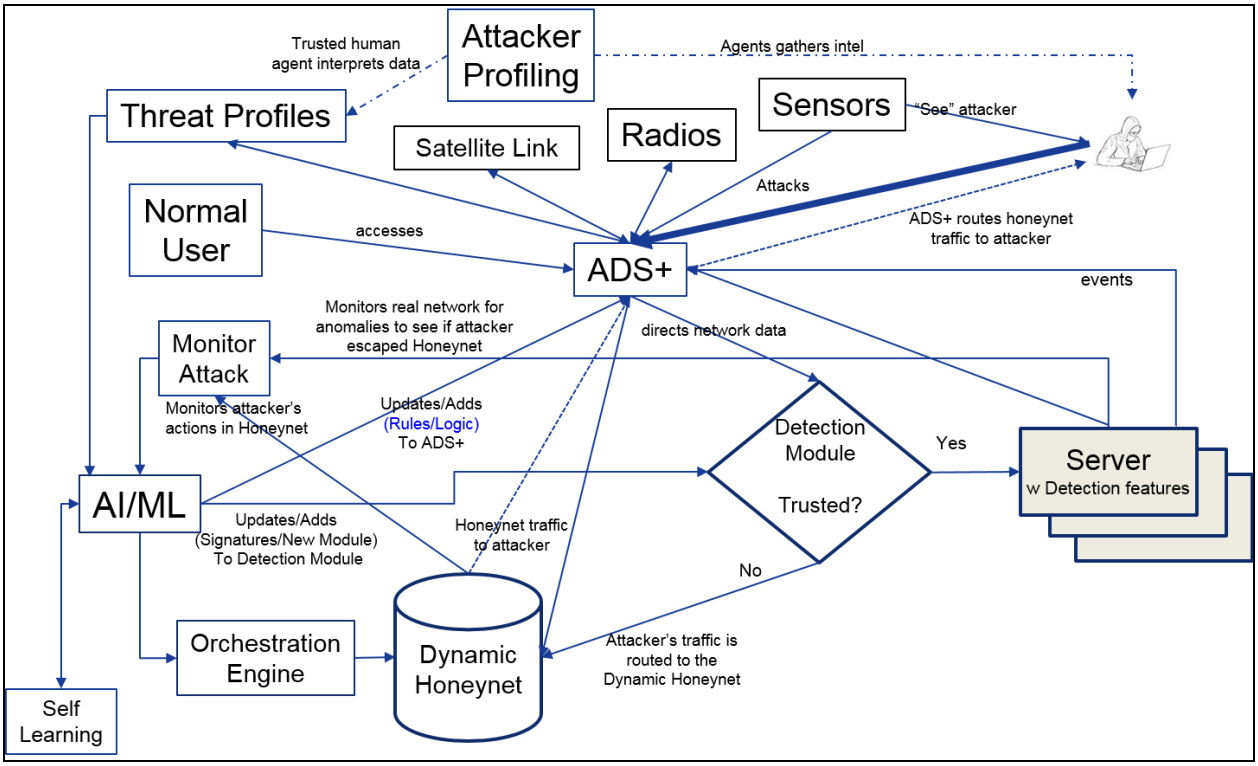

Figure 3 – Sombrero system architecture.

There are many major components in Sombrero with complex interactions, decision analysis, and various feedback paths for real-time updates. Sombrero is intended to have the ability for self-learning and to be deployed as a highly autonomous system. It will provide intelligent decisions quickly to a human operator, and/or executes those decisions automatically, especially when a cyber actor is actively attacking the system. In the following sections, we discuss details of each major component of the Sombrero defense system.

2.1 Next-Generation Active Defense System

The ADS (Active Defense System) framework for actively executing attacks against a cyber intruder has been developed at the US Army Research Laboratory (J. Acosta et al., 2016). The current version of ADS has developed a methodology that will deny, degrade, and disrupt adversary actions and expend their resources their resources. Framework components have been used to research and target malicious network traffic. It has successfully defended against a modeled data exfiltration attempt. In Figure 4, we show the current architecture of the ADS.

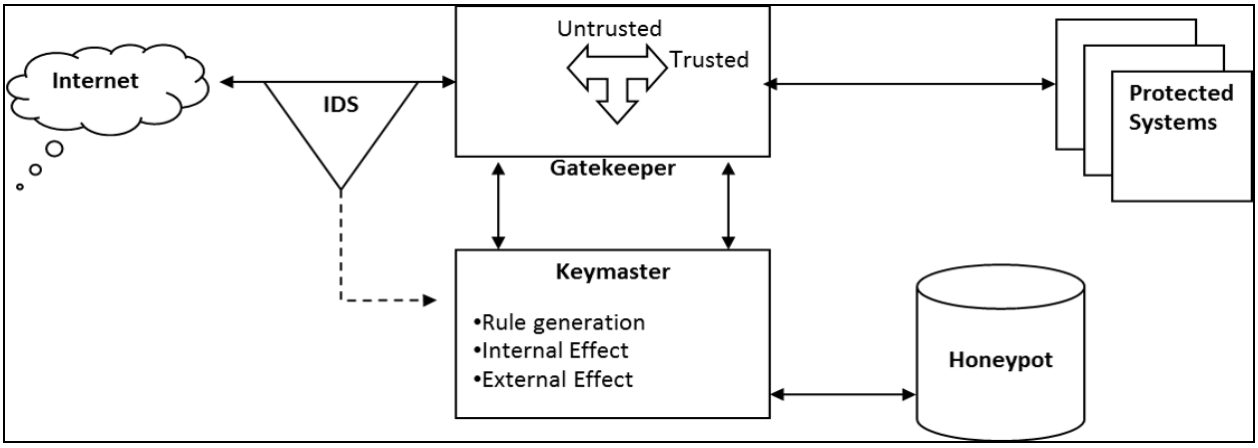

Figure 4 – Active defense system architecture.

A Next-Generation Active Defense System (ADS+) will be needed, based on the some of the technology used by the current system with more capabilities added (accepting updates from other modules, etc.) for self-updating. We next describe some of the potential features of ADS+ that would be needed for the Sombrero defense system, such as threat profiling and smart server detections. Some of the functionalities (intrusion detections, etc.) will be distributed to other modules for the purpose of separation of works. Modules can be deployed onto one server or on many servers depending on needs for survivability. Each of the ADS+ modules can handle the same types of communication or many types depending on complicity. ADS+ will serve as the gatekeeper for all network traffic in and out of the network. The incoming traffic includes sensors, radios, and satellite links, and outgoing traffic includes all internal network traffic that goes out of the network. The purpose of sensors is to detect the presence of attacker, such as motion detection of unwanted intruder, global positioning satellite (GPS) signal spoofing on the radio, etc. ADS+ also is required to validate the authenticity of the incoming traffic via certificates or other means to ensure that no one has tampered with the communication link. ADS+ needs to direct all abnormal/malicious traffic to the Dynamic Honeynet.

2.1.1 Threat Modules

The Threat Module consists of the Attacker Profiling module and the Threat Profiles module. As a feedback mechanism to Sombrero, the profile modules are used to interpret data related to information gathered about the attacker via sensors near the attacker, attacker profiles gathered from various intelligence sources, etc. When data comes from a sensor, data will be fed automatically to Sombrero. If the new information is simple, such as new attacker IP is discovered, the Threat Profile module can update ADS+ to redirect traffic of the attacker to honeynet. On the other hand, when data comes from the human sources, a threat analyst needs to interpret the results and updates the Threat Profiles module with the appropriate set of data that Sombrero understands. This module will also be used to update the Sombrero system vulnerability database once a new vulnerability is discovered.

2.1.2 Detection Module

The purpose of the Detection module is to detect incoming intrusive traffic outside of the network, prevent an attacker from accessing the trusted network (Denning, 1987), and redirect the attacker's traffic to the honeynets if found. Many AI/ML techniques can be deployed. Signature-based detection modules, such as Fast Alert Signature-based Training and Detection (FAST-D; Yu et al., 2017) will also be deployed. Anomaly-based detection using supervised learning can detect anomalous access based on historic events. Unsupervised learning can detect new indicators of compromise and attack methods. In addition, other methods can be used to detect Denial of Services (DoS) and Distributed Denial of Services (DDoS) from overwhelming our network. If DoS or DDoS attacks are detected, the traffic request can be dropped by

updates the ADS+ to remove the requested IPs. As soon as intrusion traffic is found, it will direct the traffic to the honeypot and updates rules of ADS+ to redirect the future attacker traffic to the honeynet. When no malicious incoming traffic is found, this traffic will be directed to the trusted network as intended.

2.1.3 Smart Intrusion Detection System on Servers

In dealing with insider threats and/or attack that were not caught by ADS+ and/or Detection Module, the detection features on each server can provide the capability to handle this situation. In the case of an insider attack, if the insider does not have the privilege to perform some functions or access some areas of information, an "illegal access event" will be triggered if this insider is persistently performing the illegal operations. In case an attacker was missed by the ADS+, hidden normal user decoys can be placed strategically, or an illegal access event will be triggered to redirect the attacker's traffic to the honeynet if the attacker has touched the decoy. This Smart IDS can also notify the Attack Monitor to update its database.

2.2 Monitor Attack Module

The purpose of this module is two-fold: (1) to keep track of actions taken by the attacker in the Dynamic Honeynet and (2) to monitor the internal network traffic to detect new threats that are missed by the Detection Module. Once the attacker is in the honeynets, we want to be able to track his or her steps and "bait" them to continue deeper into our honeynet. The system can then learn from his exploit methodologies and update the system vulnerabilities. If the outside attacker used valid credentials or other valid authentication means, or illegal action is generated from an insider attacker, this monitoring capability will feed back information to alleviate the corresponding shortcoming the detection module.

2.3 Artificial Intelligence/Machine Learning Module

This AI/ML module is the brain of the Sombrero architecture. It must be able to perform the following: predict human behaviors; predict his or her next move; layout a set of steps to lure the attacker to follow; keep the attacker away from the actual network; self-learn the new abnormal behavior within the network; self-learn new threats given externally that are not presently seen in the system; self-learn the attacker's new exploit methods and utilities; and self-update its own system vulnerabilities.

An Attacker Cognitive Model will be designed to predict the human behavior of the attacker. Specialized AI and ML techniques will be developed for this module. The Game Theory Model can be used as a probabilistic model to identify courses of actions based on attacker's utility. The Predictive Analysis Model will be used to predict the attacker's next move and initiate any changes any changes in the dynamic honeynet to keep the interest of the attacker to continue its course of actions. An Abnormal Behavior Model may be used to identify new abnormal behavior of the attacker. A Profile Cognitive Model can be used to learn a new threat that is learned from human inputs or external sources that are not presently used in the system. Refer to Figure 5 for data flow of the AI/ML module.

A significant amount of research and development work will be needed before the various components of this module can be properly implemented -- for example, effective human behavior and attacker profiling modeling.

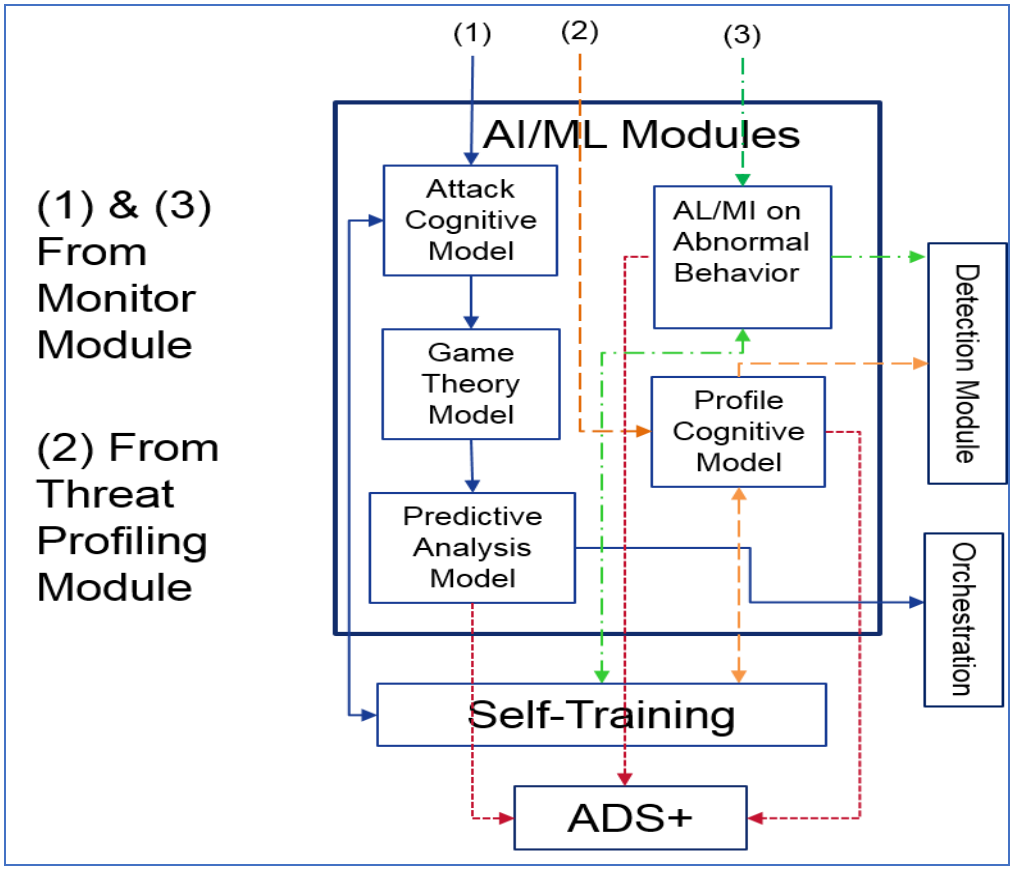

Figure 5 – Sombrero AI/ML module overview.

2.4 The Self-Learning Module

The Self-Training model is intended to be a training model that dynamically accepts real-time training data from elsewhere in the Sombrero system. Once training is done, the module will send information back to the requesting module for self-updating. This module is a container for a variety of AI/ML engines, such as reinforcement learning AI/ML algorithms to train abnormal behavior data, reinforcement learning AI/ML algorithm to train attacker profile data, and reinforcement learning AI/ML algorithms to train based on attacker's feature set. Figure 5 shows the flow of data to the Self-Training engine from various AI/ML model sources.

2.5 Orchestration Engine

The purpose of Orchestration Engine is to lure the attacker deeper into Sombrero by re-configuring the Dynamic Honeynet based on a course of action selected by AI/ML module. It will maintain or create a set of steps for the procedures for creating the next step for attacker to follow within the honeynet.

2.6 Dynamic Honeynet

The dynamic honeynet is the simulated network of the military outpost implemented by the Sombrero system. A preliminary architecture will create a small subset of virtual machine (VM) servers hosting Mission Command applications to simulate the tactical military network. It needs to have the ability to hide the facts that the VMs are not the actual system. It also needs to have the ability to dynamically create, change, and remove simulated resources, re-arrange simulated network topology, simulate operating system

(OS) footprints, and services, to minimize the ability of the attacker to access and harm vital components of the military outpost. For example, the Sombrero systems could remove a tank unit that is connected to the military outpost network if an adversary is detected. Based on the intelligent sources of a potential attacker profile, it may initialize the dynamic honeynet based on the attacker's profile interest that may attract the attacker's attention into the honeynet.

3. DISCUSSION AND CONCLUSION

As can be seen from the previous section, the complex design of the Sombrero defense system requires significant expertise from several domains. As complex as the Sombrero system will be, it must also be simple enough for a human to configure and maintain. This would need to be kept in mind when conceptual design features are proposed in the initial Sombrero architecture.

Trust and authentication are an important part of the design of the Sombrero defense system. All network traffic entering the military outpost will be validated as trustworthy by ADS+ and the Detection Module. Type-I errors (false positives) and Type-II errors (false negatives) must be minimal. These errors may be caused by an adversary spoofing non-supervised ML algorithms. An example of a Type I error is if legitimate chat messages arrive from an Army squad and they are erroneously flagged as hostile and forwarded to the Dynamic Honeynet. If these chat messages are urgently requesting support, their pleas for help will be unheard. An example of a Type II error is an enemy hacker sends bogus chat messages requesting fire support, and the messages are validated as genuine, and then friendly artillery fires upon coordinates sent by the enemy.

The game theory and cognitive models are based upon humans acting. One challenge is predicting human behavior if the enemy is not rational. We ask whether rationality can be measured? Additional research is needed in game theory, adversary cognitive modeling, and ML to realize Sombrero's goals.

Sombrero must also be aware of the local operational environment so its simulated human network traffic closely resembles the network actual messages, especially if the enemy has surveillance on the military outpost. For example, if the military network is directing artillery fire, any enemy in the Dynamic Honeynet should see messages from the compromised military operation application. Accurately modeling the types, frequency, and burstiness of each Mission Command application is important for emulating these characteristics within the Dynamic Honeynet.

Utilizing sensors to detect active countermeasures are important for congested areas such as cities with commercial and military wireless networks. Because of the high density of spectrum use, Sombrero can be an effective tool to protect the confidentiality and integrity of tactical military networks.

4. REFERENCES

[1] Alexander Kott, Ananthram Swami, Bruce J. West, "The Internet of Battle Things", Computer, vol. 49, no., pp. 70-75, Dec. 2016, doi:10.1109/MC.2016.355

[2] Chung, K., Kamhoua, C. A., Kwiat, K. A., Kalbarczyk, Z. T., & Iyer, R. K. (2016, January). Game theory with learning for cyber security monitoring. In High Assurance Systems Engineering (HASE), 2016 IEEE 17th International Symposium on (pp. 1-8). IEEE

[3] Acosta J, Edwards J, Shearer G, Parker T, Braun T, Marvel L. Modeling the decision processes of cybersecurity analysts to improve security assessments and defense strategies. Paper presented at: 23rd Annual National Fire Control Symposium (NFCS); 2016 Feb 8–11; Lake Buena Vista, FL.

[4] Denning, Dorothy E. "An intrusion-detection model." IEEE Transactions on software engineering 2 (1987): 222-232.

[5] Ken F. Yu, Nandi O. Leslie, “FAST-D: Malware and intrusion detection for mobile ad hoc networks (MANETs)”, accepted and to be published with Programme Committee of the NATO Specialist Meeting IST-145 on Predictive Analytics and Analysis in the Cyber Domain, for 10 - 11 October 2017, Sibiu, Romania.