Abusive Adversaries in 5G and beyond IoT

Sharma, V., Varghese, B., McAllister, J., & Mohanty, S. P. (2021). Abusive Adversaries in 5G and beyond IoT. *IEEE Consumer Electronics Magazine*. Advance online publication. https://doi.org/10.1109/MCE.2021.3079998

Published in:
IEEE Consumer Electronics Magazine

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Abusive Adversaries in 5G and beyond IoT

Vishal Sharma, Blesson Varghese, John McAllister
Queen's University Belfast

Saraju P. Mohanty
University of North Texas

***Abstract*—5G and subsequent cellular network generations aim to extend ubiquitous connectivity of billions of Internet-of-Things (IoT) for their consumers. Security is a prime concern in this context as adversaries have evolved to become smart and often employ new attack strategies. Network defenses can be enhanced against attacks by employing behavior models for devices to detect misbehavior. One example is Abusive Modeling (AM) that is inspired by financial technologies to defend adversaries operating with unlimited resources who have no intention of self-profit apart from harming the system. This article investigates behavior modeling against abusive adversaries in the context of 5G and beyond security functions for IoT. Security threats and countermeasures are discussed to understand AM. A complexity-security trade-off enables a better understanding of the limitations of state-based behavior modeling and paves the way as a future direction for developing more robust solutions against AM.**

I. Introduction

Future communication networks are anticipated to significantly expand for connecting many tens of billions of devices and supporting a wide range of consumer applications in healthcare, navigation and disaster management under the umbrella of the Internet of Things (IoT) paradigm [1]. The expansion is supported by 5G and technologies beyond that offer network slicing, reconfigurable connectivity, traffic steering and flexible deployment options to improve the overall efficiency of applications and minimize interference [2]. For pragmatically connecting IoT devices simultaneously over a spectrum, the response time should be ten milliseconds or lower.

Security plays an essential role in communication networks for seamlessly connecting billions of IoT devices and ensuring operational efficiency while effectively utilizing resources [3] [4]. The 3rd Generation Partnership Project (3GPP) has proposed dedicated 5G security functions that operate between IoT devices and the core. The discovery and placement of these functions, for example, the authentication server function, the security anchor function or session management function [5], is challenging and dependent on the types of applications and devices.

Behavior modeling is usually the initial step taken to evaluate whether devices work as specified, to correctly log memory and location data, and to enhance consumer trust towards the networks. Numerous strategies that use behavior models have been investigated to represent threats and adversaries in a network [6]. Abusive modeling (AM) is one strategy inspired by the domain of protocol abuse in blockchain [7] to model adversaries that simply hamper systems without wanting to obtain a profit in doing so. AM is therefore a potential candidate strategy for evaluating 5G and beyond IoT networks, given that an adversary may use unlimited resources to attack host or network-side devices. Figure 1 conceptually illustrates an architecture for the attack behaviour modeling for adversaries in 5G and beyond IoT networks. The architecture considers public and private clouds that support IoT device operations by making use of the edge. An adversary focuses on overpowering the network security functions, such as Authentication Server Function (AUSF), Authentication Credential Repository and Processing Function (ARPF), Unified Data Management (UDM), Session Management Function (SMF), Security Anchor Function (SEAF), Access and Mobility Management Function (AMF) and Policy Control Function (PCF) to adversely impact the 5G network. Manipulat-

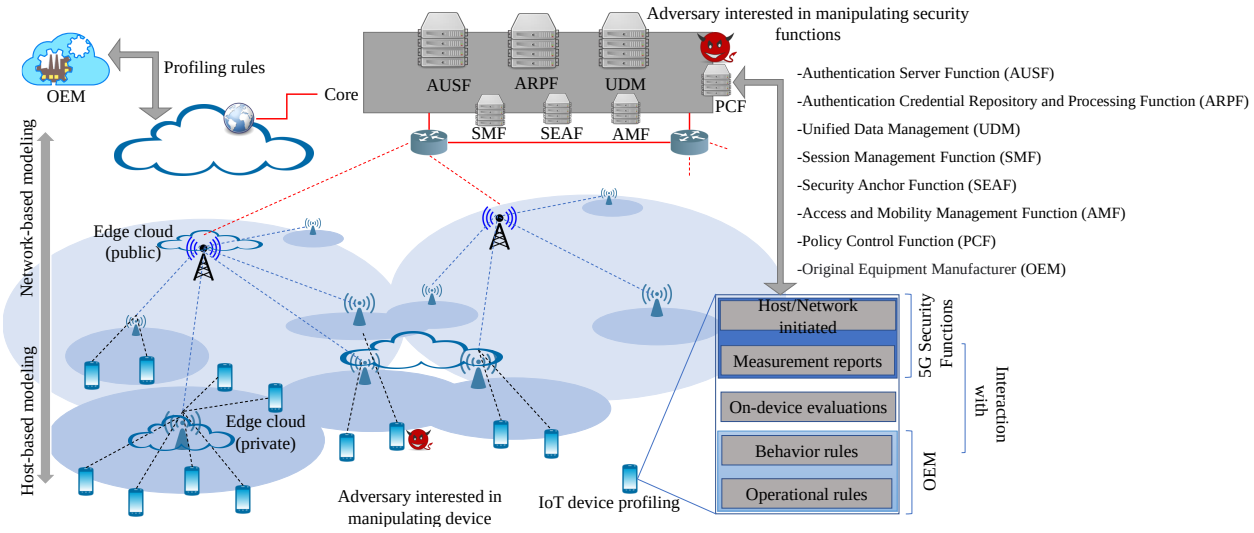

Fig. 1. An exemplary illustration of attack behavior modeling with adversaries in 5G and Beyond IoT networks.

ing these security functions require an unlimited amount of resources, which is the underlying ideology of abusive adversaries. An adversary may build strategies to attack the host or the network depending on the type of access it is able to attain in the network and the timeliness of the attack. In the case of network security functions, PCF plays a crucial role as it will decide on the interaction of IoT devices with the core. Thus, regulating the security components of the network. It is often difficult to identify whether a system is under adversarial attacks that operate with AM when it by-large controls the portion of the network or impersonates as a security function, as shown in Figure 1. However, the impact of adversaries may be limited by accurate profiling, analysing the behavior of IoT devices, and evaluating the function of protocols.

This article addresses the importance of behavior modeling of IoT devices in the context of 5G and beyond security functions. The article highlights the essentials of AM for 5G and beyond IoT systems followed by strategies of state-based attack and those factors that affect the detection of misbehavior if a system was under threat of abusive adversaries. A numerical case study is provided to understand the impact and relevance of studying AM for securing future networks and how it can pose a threat to the system if the adversaries have sufficient capabilities to control the end-devices or even the security functions that operate at the core. Furthermore, the article discusses potential solutions for mitigating the impact of abusive adversaries.

II. Behavior Analyses and Models

Existing literature presents security at multiple levels, including device to device, protocol, network, or application. Besides, working according to the behavior-rules of a connected device needs to be considered [8]. Behavior modeling is usually centralized, where a central entity holds matching rules of evaluation. Approaches adopted to mitigate the security issues in centralization include the creation of a Trusted Execution Environment (TEE) that provides a secure enclave for evaluating the behavior of the entities involved. However, decentralized verification offers the ability to independently evaluate devices by injecting *self-checking logic* into the devices [9]. Behavior modeling is complex since the types of devices vary at each deployment-level of the network [10]. Moreover, evaluating every device on pre-determined parameters (available from the product description) prohibits scalability and effective deployment of behavior models [11]. In practice, behavior models should be defined by the Original Equipment Manufacturer (OEM) of devices and third parties can help assure operations

and governance of the involved devices. The following types of analysis can be performed using behavior modeling on IoT devices that operate in the network periphery:

• **Individual analysis:** refers to the individual assessment of every device by considering operations relevant to the processing of information. This analysis is useful for monitoring a single device, which may be crucial in the network. For example, consider the use of behavior-models for analyzing access points. The volume of end devices connected to an access point may vary thus making it difficult for assessing end devices individually.

• **Group analysis:** is employed when devices operate collectively, and may or may not be connected to a common access point. The devices may have a similar profiling pattern irrespective of the make. An example is the use of network slices for managing a group of devices, and slice gateways are anchors for behavior profiling.

• **Hybrid analysis:** refers to a combination of individual and group behavior modeling. Consider a scenario in which a network slice manages multiple devices, but each device has a different make and even varying operational requirements. In this case, not only must the behavior of traffic coming off the gateways be determined, but also from the connected devices.

The above analyses can operate as

• **Sequential models:** understand devices synchronously in the order of their activity. However, these models due to cohesion are tedious to use as profiling of one device impacts other devices across the network. Therefore, sequential models cannot provide an independent assessment of the system.

• **Hierarchical models:** profile devices in a hierarchy either from a higher-end device (core) to the lower (end-user), or vice versa. The precedence and the direction of the flow of information are essential to this model. Hierarchical models support multiple layers comprising devices that are differently coordinated in the network [9]. These models lend themselves to scenarios where there is server-client activity.

• **Parallel models:** are best suited for fine-grained evaluation and formal checking of devices in the network. Having multiple inputs and outputs is an advantage of using parallel models [9].In this model, the system is divided into customized subunits to carry out parallel-profiling. This division improves the convergence and allows efficient behavior modeling even for the device to device observations.

III. Behavior Procedures for 5G-IoT

Based on the existing research [9], [12], [13], the behavior modeling workflow involves, state-machines, behavior-verification, and misbehavior detection as explained below:

A. Behavior State-Machines

It is general practice to identify states in behavior models to easily identify the processing of the information and the current device activity. By considering states, the system can express rule-based governing conditions and thereby easily identify conflicting patterns that deviate from normal working patterns. Figure 2 expresses an exemplary scenario of the state machine and its utilization in behaviour modeling. It includes a four-part state machine with a limiting number of states. The state machine can select a device, profile it, build behaviour rules based on host or network-based operations and verify the rules. 5G-PCF can handle the flow and the management of rules between the OEM and the actual IoT device. Host-based verification relies on self-checking logic whereas network-based verification relies on a separate logic checking system to be deployed within the network. However, if the number of the states are high, then the complexity of the system increases; the model will need to evaluate at least N^M states, where N is the number of outputs and M is the number of patterns associated with the behavior of the devices [12]. Nonetheless, state-based systems can be advantageous in facilitating self-checking logic on the device that is crucial for decentralizing the modeling process. Self-checking logic is an intelligent solution that can be regulated by the use of machine-learning algorithms. Machine-learning solutions play a pivotal role in establishing efficient rule-based behavior modeling with a self-checking logic.

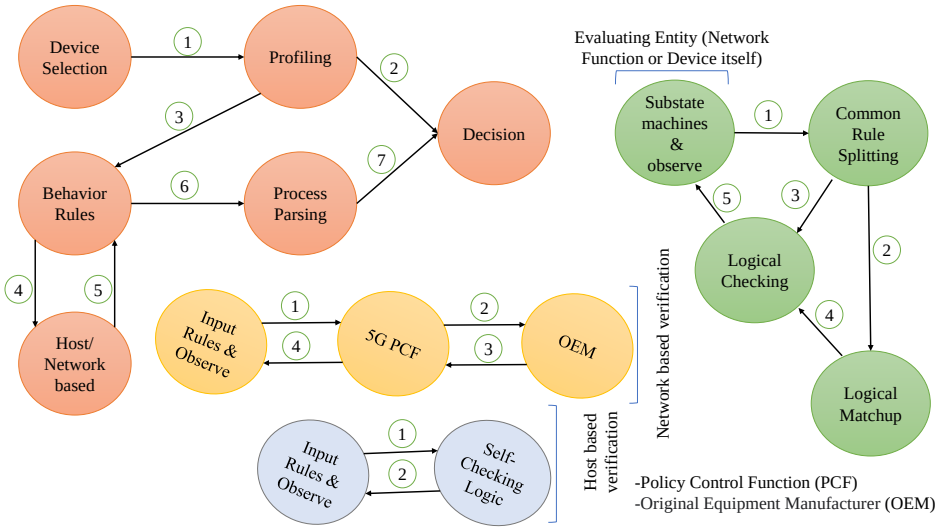

Fig. 2. State machines and behavior model verification.

B. Behavior-rules verification

In conjunction with behavior modeling, the rules defining the behavior must be verified. In other words, how can the behavior-rules defining the correct working of a device be guaranteed? Existing research presented in the literature has discussed the accuracy of the identifying rules [6], [9], [10], [12]. However, the limiting factor is usually the procedures used for checking accuracy accompanied by a static evaluation of the behavior-rules. The procedures are underpinned by state machines which leads to high complexity and slow convergence. Additionally, there is a lack of real-time formal methods to evaluate the behavior-rules. To date, behavior-rules verification employs theorem-based solutions, such as ACL2 (A Computational Logic for Applicative Common Lisp), logical forms, conjunctive or disjunctive, or offline context-matching [9].

When verifying behavior rules, high false positives need to be avoided. From our earlier discussions, whether the system will require a central entity for verification or a self-checking logic is another avenue that needs to be explored. With a large number of operating devices, self-checking is a good solution that would lend itself to decentralized-verification. However, self-checking requires a significant amount of memory and computational power, thereby limiting deployment at scale [12]. Behavior-rule verification is a necessary step in misbehavior detection since adversaries may play the system, thus, altering the rules that determine the correct working of devices. Understanding the factors of security and relating them to the behavior-rules that define a device are the steps to be carefully considered while profiling a network with a large number of connections. Once accurate profiling is attained, and behavior-rules are verified, the system can be utilized to check for any misbehavior.

C. Misbehavior-Detection

Misbehavior-detection involves the identification of outliers, threats, and vulnerabilities of a system [14]. Several methods are employed in the literature, such as signature-based, rule-based, role-based, specification-based and outlier-based approaches [13]. These are further divided into statistical and non-statistical methods depending on the type of data generated by the device [6]. The methods may be combined with AI techniques to improve the accuracy of detecting misbehavior at lower false positives and negatives. AI techniques, such as ensembles of machine learning models have been recently used to increase detection rates subject to the properties of the available data.

Another factor downplayed in the case of misbehavior detection is the mode of identification-

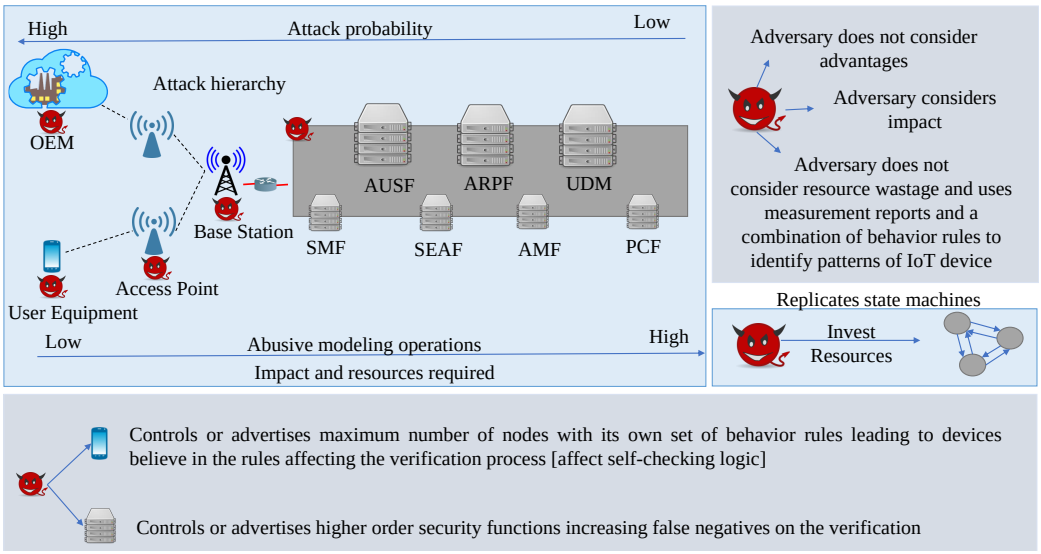

Fig. 3. An exemplar of state-replication in AM.

offline or online detection. Whether the system is deployable in real-time or requires offline processing of the available data affects the deployment of the system. In the case of IoT, online detection is important, whereas offline evaluation can only help with the future prevention of similar issues but does not provide a strong ability to have a firewall for real-time misbehavior detection.

With the utilization of 5G and beyond security functions, the detection is doable as a part of the authentication, authorization, and access control supported by the network base stations, hubs or switches. In the case of 5G-IoT networks, the positioning of the security functions plays a pivotal role in deciding the risk associated with misbehavior detection. Moreover, which security functions are to be responsible and configured as a part of behavior verification are to be decided as a part of network planning. In addition, the mobility and positioning of devices in the networks need to be considered as it impacts detection of adversaries. Once a device moves across a network, its profile may change due to a change in its role. In different settings, anchor functions may not identify the device, and this impacts the detection. A device may turn rogue by helping another device camouflage within the network despite having a strong detection strategy. Thus, misbehavior detection needs further exploration considering recent drafts on several application-specific protocols for devices enabled with 5G and beyond technologies.

IV. Abusive Modeling (AM)

AM refers to when adversaries go beyond soft limits (limited resources for attacking) set for attacking and will invest in a significantly large amount of resources to cause maximum harm. In AM, the threat model may consider network entities that go rogue randomly, allowing minimum chances of recovery. More specifically, a set of IoT devices may be impacted by a common access point that behaves like an abusive adversary. Under such circumstances, the network will have a single point of failure. An adversary may have the capability to control base stations that may affect the entire front haul and mobility of devices leading to several attacks, such as host-impersonation, replay attacks, Denial of Service (DoS), Distributed Denial of Service (DDoS), hidden-terminal, in the network, as shown in Figure 3. Figure 4 helps to understand the security properties, threats and mechanism of attack in AM. The figure presents the security properties, which are the potential targets for an adversary in AM categorized concerning the host or network-based deployment. This illustration lists several attacks on the state-machines with a direction of research on misbehaviour detection.

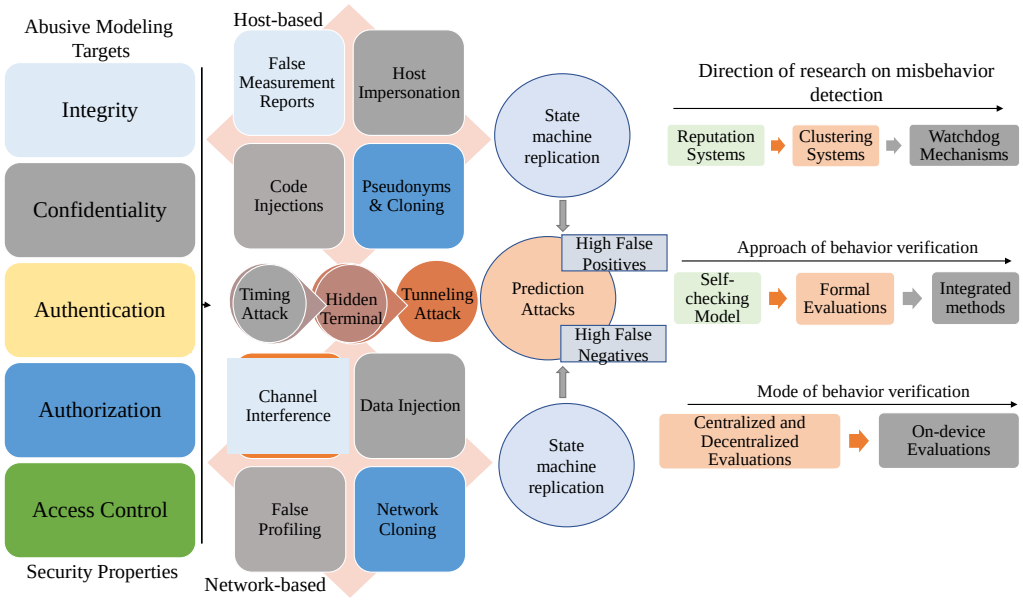

Fig. 4. Security properties, threats and mechanism of attack in AM.

State-of-the-art has identified strategies that may create abusive adversaries with maximum impact on the performance of the network. These strategies include the use of decision processes, like Markov modeling, recognition-primed modeling, agent-based modeling, and social modeling. These approaches define adversaries with AM to evaluate highly complex systems, such as 5G and beyond IoT networks. Network replication, cloning, device-injections, prejudice selection of routes, and route-forgery are strategies that are opted by an adversary operating in AM. One example is having a rogue new access point or base station when a device is moving between a previous and a new access point. If an IoT device is unaware of the rogue new station, it may provide the details of the entire network, such as exposing the previous keys, de-registration process, the timing of the sessions, and locations used for credential management. More severely, it can expose historical data that leads to multiple issues related to privacy and data integrity.

A. *Factors Affecting AM-Misbehavior Detection*

Adversaries following AM principles may override behavior rules and generate high false negatives resulting in vulnerabilities that if left undetected may lead to zero-day attacks. Furthermore, AM can delay the release of security-patches to the affected parties lowering the Window of Vulnerability (WoV). Hence, misbehavior detection techniques cannot be accounted for in real-time. Such a technique, in return, increases the cost of evaluations and overheads as most analyses of the devices will need to be repeated in an offline mode; this is inherently centralized. Thus, a decentralized setup is converted to a flat architecture resulting in issues related to mobility management, protocol violation, loss of accessibility and authorization, and authentication and access control. The following is a list of factors that may affect misbehavior detection against AM:

- **Associative-density:** refers to the inter- and intra-dependencies of devices. Since a large number of devices operate in the periphery of each other, abusive adversaries may have multiple entry points to the system and can manipulate rules or inject their own rules to change the governing conditions that identify misbehavior. The degree of control by the abusive adversary directly impacts detection and control over the network. With a high number of compromised devices, the detection is affected, and the probability of identification decreases.

- **Architecture:** Whether a network is operational in a centralized or a decentralized model can de-

termine the possibility of detecting misbehavior against AM. In a flat architecture, there are multiple single points of failure for a subset of devices. Under such conditions, abusive adversaries will camouflage that result in high false negatives when detecting anomalies. The positioning of security functions also affects detection against abusive adversaries since the devices acting as a potential candidate for 5G and beyond security functions may not be secure enough or are under a direct attack.

• **Mobility policies:** Devices moving across terminals need to have a secure method of registering and de-registering devices with old and new terminals, respectively. If a terminal is controlled by an adversary with AM, then it may expose the entire history of the session, thus affecting the data integrity and privacy of the network.

• **State-machine complexity:** AM may fail if the number of rules defining a system is large since an adversary will need to identify many states before generating a strategy for attacking the system. With a fewer number of states, easy to execute rules, or simple threshold-based variations, AM can have much impact and control over the network and its components.

B. Impact of AM on 5G-enabled IoT

This section presents the impact of AM on 5G-enabled IoT devices by considering the states that are determined by behavior-rules.

Complexity-security trade-off: For a complex system in behavior modeling, a large number of states will need to be processed to evaluate the system. This impacts system performance. Hence, the aim of further research should be to derive solutions for rule-verification and adversary identification that can operate with sufficiently low overheads by only using a limited number of states. In other words, the complexity of the system needs to be controlled. If an abusive adversary operates in a network, then it will have to execute a large number of states for replicating the network setup before considering strategies to launch an effective attack. This can prove to be cumbersome for an adversary to launch a timely attack. However, if costs were not a concern for an adversary, then it can launch a state-wise attack. Thus, there exists a complexity-security trade-off – it is necessary to have a low complexity system for rapidly verifying a system with only a few states, but at the same time complex state-based verification does not naturally lend itself to adversarial attacks.

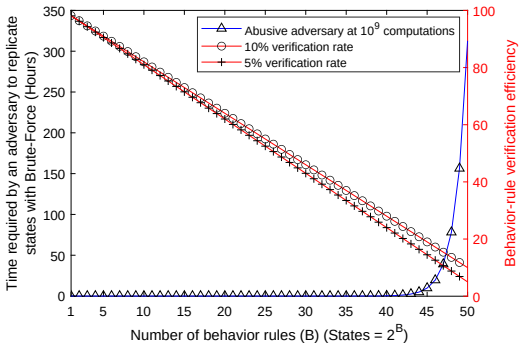

Fig. 5. Complexity-security trade-off to understand the impact of AM.

The article presents a case study of an adversary having the capacity to perform fast computations under no monetary cost constraints. For the sake of simplicity, the system used is assumed to be operational on binary output with each behavior rule resulting in two states. The types of behavior-rules are not considered at present and evaluations are limited to their number rather than the type of behavior-rules and will be considered in the future. The graph illustrates that by having multiple states representing multiple behavior rules will increase the verification complexity of the system. The total number of operational-states increases in the order of 2^B, where B is the number of behavior rules. If an adversary has the capacity to operate a billion computations per second, then a brute force attack can be launched by using a trivial multiplicative inverse to replicate the exact states of the system (shown in Figure 5). The numerical results suggest that the time to replicate the states by an adversary increases with an increasing number of behavior-rules. However, with this increase in the number of rules, the verification-rate decreases, i.e., the rate at which the system can verify all states/rules of the system decreases thereby making the system less effective in detecting abusive attacks. It decreases the efficiency of the entire system in detecting AM attacks.

Induced failures by AM: Abusive adversaries

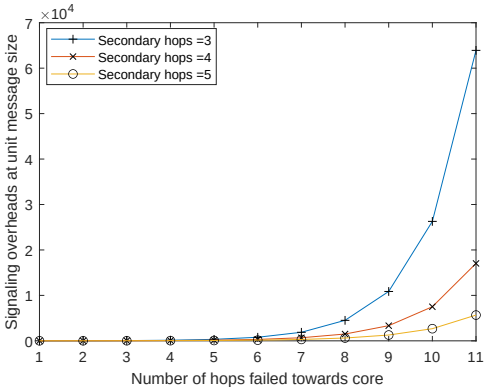

Fig. 6. Signaling overheads versus hop failure with respect to network density.

can use unlimited resources to either compromise the host IoT device or 5G security functions. Its impact depends on network depth and network density. If the number of secondary devices (alternative routes with additional devices) is large, then the network may be able to regulate traffic for preventing a state-based attack. However, if the adversary controls the security function in the network, then the failures of entities increase. Such types of failures and increase in load on entities are traceable by calculating signaling overheads using formulation in [15]. An adversary, controlling the network functions that are required for secure working of the communication protocols, will induce overheads either on the host-side or directly on the network-side. In our impact evaluation, the network considers unit message size to understand failures that are expressed to understand the general impact on the system as signaling overheads, as shown in Figure 6. The network utilizes security functions operating with 10 to 30 nodes and the number of hops that fails ranges between 1 and 11. The security functions are placed at the wide-end of the system. The failing hops are considered for both the host-side as well as on the side of the security functions. With decreasing neighboring nodes (between 3 and 5), the signaling overheads increase rapidly resulting in several failures. It is now evident that an abusive adversary severely impacts the system. Thus, it is necessary to explore strategies that can address the implications of AM where location-privacy needs considerable attention to prevent state-replication under AM.

V. Prospective Solutions

Potential solutions (as shown in Figure 7) against AM with their limitations are discussed below:

- The generation of operational profile of devices that cannot be easily carried out manually can be automated using ML to extract behavior-policies. With advanced grade-sensitive tools, even devices that merely have input/output roles can be associated with a set of criteria to fix their behavior patterns. Automated patterns with ML can help in efficient mining, detection, filtering of outliers, and anomaly detection.
- The state-replication by abusive adversaries can be overcome by increasing the secret sharing of data. Stronger encryption can provide security against AM, although it will increase the overheads for the devices to process the incoming data. This leads to another security-efficiency tradeoff that can be explored further specifically targeting state-replication. Group Authentication can be an effective solution, and in the case of 5G-IoT, slicing and authenticating the group of devices is an efficient mechanism given the advantages of pre-build security functions.
- Approaches like Markov Modeling, Optimal Stopping theory, and Transfer Learning can be used to develop a new set of strategies to evaluate the convergence, responsiveness, and sensitivity of formal verification of behavior rules against AM. These can overcome the complexities associated with the verification as the actions can be set to decrease the number of verifiable states. However, the performance overheads of these approaches is a disadvantage to be resolved.
- Filtering techniques, such as Kalman filters, $\alpha - \beta - \gamma$ filters, and optimization solutions, like nature-inspired algorithms that have low turnaround time can be used atop of formal verification to support the misbehavior identification at lower false positives.

VI. Research Directions

The following avenues of research are recommended for further exploration to understand the impact of AM for behavior evaluations of IoT:

- It is required to understand the decision-making on the location of state-machines and approach for

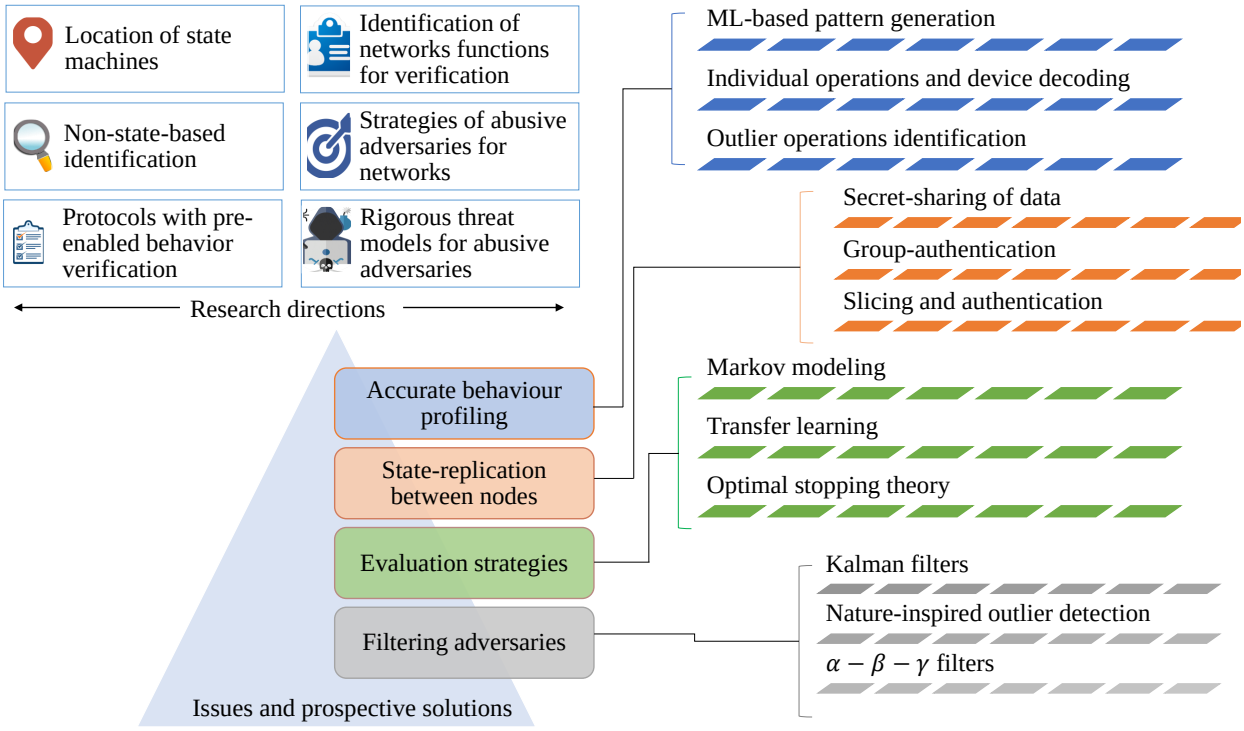

Fig. 7. Prospective solutions and research directions to explore for AM in IoT.

sharing verifiability of the behavior-rules. Positioning is a dominant factor as it directly affects the devices as well as the security functions of the network.

• It is required to understand formal methods as well as derive new solutions that can help generate true-states of the network. Precisely, energy constraints of the IoT devices need to be taken care of when developing such methods.

• AM does not bound to a few strategic approaches. It is still a wide-open problem, and there are no direct models that can help decide the properties of abusive adversaries focusing on network entities only. Although Markov Models can drive AM in blockchain analysis, from the network's point of view, the number of states also affects the performance and verification. Thus, it is interesting to follow and understand how futuristic approaches tackle these issues.

• Incorporating security functions with additional properties to have a pre-embedded mechanism of behavior verification, along with authentication, is another direction to explore. Moreover, a new security function can follow to dedicatedly verify the behavior and run in parallel to overcome performance issues.

• Rigorous mathematical models can help to form a common threat model that takes into consideration the process or strategies of AM when evaluating security solutions for 5G and beyond IoT networks.

VII. Conclusion

Behavior modeling is pivotal for understanding new types of attacks in 5G and beyond IoT since adversaries are becoming intelligent. This paper presented abusive modeling (AM) as a worthy area of exploration to mitigate attacks when an adversary has an unlimited amount of resources to launch an attack. The benefits of exploring AM for IoT networks are obvious but relatively new compared to its use for protocol abuse in financial technologies, such as blockchain. The article presents the limitations of existing behavior modeling techniques, state machines, and how they impact the performance of the network, and misbehavior detection within the context of a complexity-security

trade-off discussed using a numerical case study. Given the severity and negative consequences of abusive adversaries, further research is required on efficient behavior rule verification, prevention of state replication, and secondary network for load-balancing in the case of attacks to develop robust and counter solutions.

REFERENCES

[1] F. J. Dian and R. Vahidnia, "LTE IoT technology enhancements and case studies," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 49–56, 2020.

[2] D.-Y. Kim and S. Kim, "Network-aided intelligent traffic steering in 5G mobile networks," *Computers, Materials & Continua (CMC)*, vol. 65, no. 1, pp. 243–261, 2020.

[3] S. U. Malik, "Moving toward 5G: Significance, differences, and impact on quality of experience," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 9–14, 2020.

[4] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection in smart home operation from user behaviors and home conditions," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 183–192, 2020.

[5] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization, and research directions," *IEEE Network*, vol. 34, no. 5, pp. 306–314, 2020.

[6] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 779–811, 2019.

[7] P. Szalachowski, D. Reijsbergen, I. Homoliak, and S. Sun, "Strongchain: Transparent and collaborative proof-of-work consensus," in *Proceedings of 28th {USENIX} Security Symposium*, pp. 819–836, 2019.

[8] J. Ortiz, C. Crawford, and F. Le, "DeviceMien: Network device behavior modeling for identifying unknown IoT devices," in *Proceedings of the International Conference on Internet of Things Design and Implementation*, p. 106–117, ACM, 2019.

[9] V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems," *IEEE Access*, vol. 7, pp. 118556–118580, 2019.

[10] J. Sun, W. Shi, Z. Yang, J. Yang, and G. Gui, "Behavioral modeling and linearization of wideband RF power amplifiers using BiLSTM networks for 5G wireless systems," *IEEE TVT*, vol. 68, no. 11, pp. 10348–10356, 2019.

[11] D. Li and J. Zhong, "Dimensionally aware multi-objective genetic programming for automatic crowd behavior modeling," *ACM Trans. Model. Comput. Simul.*, vol. 30, no. 3, pp. 1–24, 2020.

[12] G. Choudhary, P. V. Astillo, I. You, K. Yim, R. Chen, and J.-H. Cho, "Lightweight misbehavior detection management of embedded IoT devices in medical cyber physical systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2496–2510, 2020.

[13] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, pp. 1–29, 2014.

[14] N. V. Abhishek, A. Tandon, T. J. Lim, and B. Sikdar, "A GLRT-based mechanism for detecting relay misbehavior in clustered IoT networks," *IEEE Transaction on Information Forensics and Security*, vol. 15, pp. 435–446, 2019.

[15] I. You and J.-H. Lee, "SPFP: Ticket-based secure handover for fast proxy mobile IPv6 in 5G networks," *Computer Networks*, vol. 129, pp. 363–372, 2017.

ABOUT THE AUTHORS

Vishal Sharma is with the School of Electronics, Electrical Engineering and Computer Science (EEECS) at the Queen's University Belfast (QUB), NI, United Kingdom. Contact him at: v.sharma@qub.ac.uk.

Blesson Varghese is with the School of Electronics, Electrical Engineering and Computer Science (EEECS) at the Queen's University Belfast (QUB), NI, United Kingdom. Contact him at: b.varghese@qub.ac.uk.

John McAllister is with the School of Electronics, Electrical Engineering and Computer Science (EEECS) at the Queen's University Belfast (QUB), NI, United Kingdom. Contact him at: jp.mcallister@qub.ac.uk.

Saraju P. Mohanty is the Editor in Chief of the IEEE Consumer Electronics Magazine and Professor in the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. Contact him at smohanty@ieee.org.