Review on the Composition : " A Novel Method for Intrusion Detection in Autonomous Distributed IoT Systems Utilise Stochastic Petri Net Modeling"

Mr. Pradeep Nayak, Mr. Darshan K Revankar, Mr. Gautham P Kini, Mr. Yashash Raj C G, Ms. Dikshita Devadiga

pradeep@aiet.org.in , darshankrevankar@gmail.com , gautham07049@gmail.com , yashash426@gmail.com , dikshitadishu8@gmail.com
Department of CSE (IoT, Cyber Security including BlockChain)
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India

ABSTRACT

The integration of an Intrusion Detection System (IDS) in Autonomous Distributed IoT Systems (ADIoTS) plays a crucial role in enhancing cybersecurity by addressing challenges such as insider attacks, Byzantine failures, and energy efficiency. This research proposes a Stochastic Petri Net (SPN) model to simulate and evaluate the system's performance. A collaborative security framework, supported by a voting system, is introduced to improve anomaly detection and system longevity. The proposed approach ensures a robust and resilient IoT environment, enhancing the overall cybersecurity posture while maintaining efficiency and reliability in distributed autonomous systems.

Keyword : -*The integration of an Intrusion Detection System (IDS) in Autonomous Distributed IoT Systems (ADIoTS) enhances cybersecurity, focusing on insider attacks, Byzantine failures, and energy efficiency. A Stochastic Petri Net (SPN) model, along with a collaborative security framework and voting system, ensures anomaly detection, system longevity, and cybersecurity resilience.*

1. Introduction

This paper addresses the meaning challenge of securing Autonomous Spread Internet of Things (ADIoTS) system of rules, which are increasingly utilized in critical environments like military operations, disaster recovery, and remote monitoring. A major security consequence for ADIoTS is the hazard of insider attacks, where compromised nodes can peril the system 's integrity and disrupt its functioning. These system are urinate up of autonomous, military mission - driven IoT devices — such as detector, actuators, and control nodes — that collaborate to accomplish specific objectives. Leave their decentralized structure and the diverse task they handle, ensuring the security department and reliability of these organisation is vital. < /p>

To tackle these issues, the paper presents a new approach that integrates Intrusion Detection Systems (IDS) at each lymph gland within the ADIoTS meshing. This is all important because traditional centralized security system measures may fall scant in such distributed and dynamic environs. Instead, the paper proposes a collaborative security framework where each node is tax not only with its designated mission but also with identifying and defending against potential intrusions. This three-fold role assure that every node actively bring to uphold the system 's unity while fulfil its principal mission.

A key creation in this approach is the use of Stochastic Petri Net (SPN) modeling, a robust mathematical technique that effectively represents the complex, stochastic doings of the organisation over time. SPN is particularly skillful at modeling the dynamic interaction between attack and defense strategies in a distributed surroundings. By utilizing SPNs, the paper introduces an analytical framework that can predict and optimise defense lawyers strategy for each node, enable them to pad their resiliency against blast while maximizing the arrangement 's operational lifespan.

This methodological analysis underline detect the optimum configuration of defense parameters, such as the oftenness of intrusion detection (sensing separation, TIDS) and the turn of voting lymph gland involved in the collaborative determination - making operation. These parameters are crucial for equilibrate the business deal - off between the effectivity of intrusion detection and overall imagination usage, admit energy ingestion, within the system. By leverage SPN models, the paper propose to ensure that the ADIoTS can endure various case of malicious attacks — whether persistent, opportunist, or strategic — without compromising its missionary post objectives or longevity.

In essence, this paper not merely introduces a new IDS design for ADIoTS but also offer up a methodology that assure the system remains secure and operational over time, still in the face of insider threats. The proposed glide slope financial aid in optimizing Department of Defense strategies, thereby raise the resilience and lustiness of Autonomous Distributed IoT organization in mission - vital surround, where certificate and system uptime are of utmost importance.

ADIoTS System Model

The Autonomous Distributed Net of Things (ADIoTS) simulation is designed around mission - oriented IoT devices. Each device, or node, possess the dual role of execute its specific task — such as sensing, actuation, or communication — while also handling Intrusion Detection System (IDS) responsibilities. This combination insure that every guest plays a constituent in assert the overall security measure of the system while executing its primary function. Nevertheless, these nodes are particularly vulnerable to capture attacks, where an attacker can breach a lymph node 's protection, acquire access code to sore information or the internal network of the organisation. Once compromised, these nodes can become insider threats, enable attackers to manipulate the system of rules from within. They may give accession to security tonality, confidential data, or the capability to interrupt operations without detection. Consequently, the organization must contend with not entirely external threats but also home dangers posed by compromised nodes.

To find insider threat and asseverate scheme integrity, Intrusion Detection Systems (IDS) are regularly put through at each client, where they monitor and value the demeanour of neighboring nodes. Each node casts a vote on whether its neighbors are act as appropriately (voting " yes ") or unsuitably (vote " no ") based on their observations. This ballot system is essential for name compromise nodes and ensuring early sleuthing of malicious action. However, malicious nodes can take advantage of this collaborative voting by utilise delusory strategies like ballot stuffing and badmouthing. Voting stuffing find when malicious node vote " yes " for themselves or for other malicious nodes, falsely presenting them as legitimate participants. Conversely, drag through the mud involves malicious node vote " no " for lawful nodes, incorrectly branding them as misbehaving. Both tactic can severely skew the voting process, ensue in wrong conclusion that misidentify malicious nodes as harmless and logical nodes every bit harmful. Consequently, the organization 's electrical capacity to detect attacks and uphold operational integrity is undermined, potentially diminish the organization ’s lifespan and effectiveness.

The likely failures that can occur within an ADIoTS are classified into several types, each of which can significantly touch the system of rules 's overall functionality and commission success:

1. Byzantine Failure : This type of loser arises when consensus go unattainable due to a declamatory number of compromised nodes. In a Byzantine failure scenario, legion node may pretend maliciously, take to conflicting voting and making it insufferable to agree on the trustworthiness of any specific node. This failure can endanger the full IDS mechanism and disrupt system operations.

2. Attrition Failure : This failure go on when a significant number of nodes are compromised or disabled, leave in an insufficient number of functional nodes to perform the organization 's tasks. In mission - critical systems, especially those deploy in essential applications, birth a sufficient telephone number of operational knob is crucial to accomplish overall chore prerequisite. If grinding slim the number of functional nodes below a critical grade, the arrangement may be unable to complete its mission.

3. Resource Depletion Failure : Each lymph node in the organization has limited resources, in particular regarding energy. As nodes carry out IDS tariff periodically, their energy usance addition, and they may finally wipe out their power supply. When client can no more long engage due to energy enervation, the system of rules may live a diminished capacity to notice and respond to blast, or worse, fail to gather task requirements entirely.

4. Coating Failure : This occurs when the system can not fulfill its project requirements, still if a sufficient number of nodes remain operable. Covering failure can result from nodes that, while functional, are unable to execute their assigned chore due to interference, erratic behavior, or inaccurate attack detection.

The strategy utilise by malicious role player to attack organization are divers and specifically designed to work particular vulnerabilities:

1. Persistent Approach : These involve a long - term commitment to compromise or break up the organisation. Malicious nodes may consistently target sure leaf node, seek to breach IDS defenses over time.

2. Random Attacks : In these pillowcase, the aggressor ’s action mechanism are unpredictable. Malicious knob can strike at any moment, making it more intriguing for the IDS to detect and respond to these threats. Random onset take up advantage of the organization ’s inability to envision attacker behavior.

3. Opportunist Plan Of Attack : These attacks hold back for the consummate here and now to occur. Malicious nodes may focus on nodes that are vulnerable ascribable to external constituent (like humble Energy Department) or internal circumstance (such as lessened corporate trust layer), but only when the opportunity for successful disruption arises.

4. Selective Attacks : These are strategically aimed at specific lymph gland, often those with expectant potentiality or critical subroutine within the organisation. By target high - time value node (for illustration, those responsible for indispensable tasks or containing full of life datum), the attacker seeks to make maximum perturbation to the system ’s overall performance.

To address the diverse and intricate attack scheme, justificatory amount are crafted found on the bit of ballot nodes and the intervals for intrusion detection (TIDS). The voting arrangement calculate on having enough guest involved in the conclusion - making cognitive process to attain a consensus reckon the demeanour of their peer. The quantity of voting nodes (m) act as a all-important theatrical role in the succeeder of flak spying, as a capital issue of voters can lessen the influence of malicious nodes trying to shake the voting process. Besides, the intrusion detecting interval (TIDS) dictate how oftentimes nodes monitor for attacks and make vote selection. Fine - tuning TIDS is essential to balance system resource usance (like energy and processing power) with the need for well-timed onslaught detection.

By thoughtfully adjusting these parameters, defensive scheme target to counteract fire method acting and stretch out the system ’s operational lifespan. With these adaptive defence mechanism strategy, the organization is easily outfit to live on a range of attack scenarios, subjugate the chances of failure while achieving its mission finish. At Long Last, the objective is to create a racy ADIoTS that can function effectively still when face with modern insider and outsider menace, ensuring the durability and succeeder of mission - vital IoT systems.

Evolution and Optimization of Defense Strategies

The paper put in a **robust Intrusion Detection System (IDS) framework** that is implemented at every lymph gland within the Autonomous Distributed Internet of Things System (ADIoTS). The chief objective of this framework is to maximize the system 's Mean Time to Failure (MTTF) by efficaciously fend for against potential cyber menace and check the organisation ’s continued functionality. To accomplish this, the authors use Stochastic Petri Net (SPN)-based models to rigorously psychoanalyse various defense strategies that can be deployed at the node floor. These models help simulate the complex dynamics between attack and defensive structure within the ADIoTS, focusing on cardinal parameters that influence system performance and security, such as the **detection separation (TIDS)** and the **number of voting node (m)**.

The **detective work musical interval (TIDS)** advert to the periodic interval at which nodes fulfill their IDS obligation, notice possible intrusions and put votes about the behavior of their neighbors. The balloting knob (m), on the former hired man, are the subset of nodes responsible for for determining the authenticity of former nodes ground on their mention behavior. An optimal combination of these two factors— **TIDS** and **m**—is of the essence to achieving the best performance in terms of both attack detection and **system of rules longevity**. If detection intervals are too forgetful, nodes may squander overweening resources, subjugate energy and performance efficiency. Conversely, if the intervals are too prospicient, there might be delays in detect malicious action, lead to a compromise in organisation integrity. Similarly, having too few ballot client can allow malicious actor to influence the voting process, while too many leaf node can unnecessarily increase system overhead. Therefore, the extract of these argument is key to balancing resource usage with effective defense capabilities.

Through the lotion of **SPN models**, the report investigates how different defense conformation affect the arrangement 's overall **MTTF**. It identifies the most prejudicious attack strategies—such as relentless attacks, random attacks, **timeserving attacks**, and selective attacks—which can exploit vulnerabilities in the system and reduce the usable liveliness of the ADIoTS. For model, dogged onslaught aspire to ceaselessly compromise lymph node over a prolonged period, wearing down defenses and causing cumulative damage. Random tone-beginning, by their unpredictable nature, challenge the IDS scheme 's ability to discover intrusions in a timely manner, while opportunistic attacks target specific weaknesses in the scheme only when the term are favorable. Selective onset, by compromising high - potentiality nodes, can cause disproportionate harm to the system 's ability to make out critical tasks.

In reception to these scourge, the author propose tailored defense strategies that are specifically designed to weaken the most harmful flack tactics. These strategies swear on conform the TIDS and **voting nodes (m)** to enhance the detection of malicious natural process while minimizing system exposure. By optimizing these parameters, the defence mechanism mechanisms can keep or extenuate the effectiveness of various attack strategies, in the end control the **length of service and reliability** of the ADIoTS.

What Is More, the newspaper spotlight the grandness of deliberate both the defense capability of individual thickening and the **attempt capability** of adversaries when designing a lively system of rules. A node 's defense capacity is shape by its ability to discover intrusions, vote accurately, and maintain operational efficiency over time. On the other hand, the attack capability refers to the sophistication and persistence of malicious worker attempting to disrupt the system. The interplay between these two factors plays a significant role in determining the system 's overall lifetime. A scheme with weak defenses is more probable to flush it prematurely, while a system with strong defenses can die hard longer, still under persistent and sophisticated attacks.

To optimize system of rules operation and decoct the risks get by these attempt scheme, the source emphasize the need for thrifty natural selection of the TIDS and **m** value. The optimal configuration of these parameters see that the arrangement remains responsive and efficient in detecting and responding to threats while maintaining the **MTTF**. Ultimately, this employment provides a foundation for contrive adaptive, resilient IDS mechanisms that can scale to come across the need of bombastic, pass on IoT systems like ADIoTS, safeguard them against a all-encompassing raiment of potential threats.

Future Work and Testbed Implementation

The author recognize that the landscape of cyber terror is incessantly acquire, and as such, they stand for to **carry their research** by bring in more **advanced onset scenarios**, particularly **collusion** and **strategic attacks**, which will render a more comprehensive valuation of the robustness and resilience of their project **Intrusion Detection System (IDS)** within the Autonomous Distributed Cyberspace of Things System (ADIoTS). Collusion attacks involve multiple malicious lymph node working together to coordinate their actions, thus evading detection by the IDS, while **strategic attacks** quarry vulnerability in the defense mechanisms themselves, often exploiting helplessness in the ballot - based detecting system or manipulating the defense strategies in subtle ways. These character of flack are specially difficult to detect and defend against, and their presentation will test the system 's ability to withstand complex, collaborative adversarial behavior. By integrate these innovative onslaught scheme, the source train to **tenseness - mental test the system** and far enhance its capacity to maintain in operation wholeness and maximize **Mean Metre To Failure (MTTF)** under a broader grasp of approach conditions.

To Boot, the source project to **refine** the existing SPN - establish models to incorporate these more sophisticated approach strategy. They pick out that the current models volunteer valuable insights, but as the attack landscape becomes more complex, thence to a fault must the mold techniques. By acquaint **increased complexity** into the models, the author will be able to simulate a wider array of attack and defense scenario, check that their findings are to a greater extent representative of actual - world challenge. This refinement mental process will too involve a more detailed complexity analysis, which will sharpen on understand how the arrangement ’s behavior alteration in response to diverse attack conditions, and how the arrangement ’s Defense strategy can be optimized for greater efficiency and effectiveness. Through this work, they desire to produce to a greater extent robust, scalable defense reaction mechanisms that can handle emerging threats and avail IoT systems stay on inviolable in dynamic, material - world environments.

To **validate the results** obtained from their analytical models and see the practical pertinence of their findings, the generator declare oneself the development of a real - existence testbed draw up of **128 mobile sensor nodes**, which will be free-base on Raspberry Pi devices. These devices will be equip with lightweight IDS hosts capable of perform **anomaly detection** and **intrusion detection** tailored to the specific pauperization of IoT environment. Each client in the testbed will dish out as both a **missionary post - oriented** node and an intrusion detection node, allowing the author to simulate substantial - human race conditions in which nodes not only perform their assigned labor but also get together with neighboring nodes to detect and neutralize potential threats. By enforce the suggest defense strategies on the testbed, the writer will be able to accumulate empirical data on the system of rules ’s performance, including the **accuracy** of the IDS in discover blast, the **resource consumption** required for defense operations, and the **system ’s overall longevity** under various attack scenarios.

This substantial - world testbed will be instrumental in validating the effectiveness of the proposed **collusion - aware vote - based IDS (CAVBIDS)** design, cater empirical evidence to abide the analytic determination and demonstrate the **feasibility** of the defense mechanism in pattern. The testbed will also enable the generator to assess how well the **SPN - ground models** align with actual system behavior and to stimulate adaption to improve the model ’s prognostic power. By meld theoretical models with **empirical data**, the writer aim to create a more comprehensive and dependable framework for securing Autonomous Distributed IoT Systems against a wide range of likely threats.

Ultimately, the development of this testbed and the validation of the **analytical models** through real - world experimentation will secure that the suggest defense team strategies are not only theoretically sound but besides **practically viable** for deployment in real IoT systems. It will also pave the mode for future research in this plain, enabling the generator to try out more advanced plan of attack scenarios and continually fine-tune their models to treat the acquire nature of cybersecurity scourge in Autonomous Distributed IoT environments.

Conclusion

In conclusion, this paper give a novel approach to raise security system in Autonomous Distributed Cyberspace of Things Systems (ADIoTS) through the integration of Intrusion Detection Systems (IDS) at each node. The

proposed fabric utilise Stochastic Petri Net (SPN) manakin to capture the dynamic interaction between attack and defense force strategies, aiming to maximise the system 's Mean Time To Failure (MTTF) under diverse onslaught conditions. The field foreground the importance of select optimal Defense Department argument, such as detection intervals (TIDS) and the issue of voting nodes (m), to ensure system longevity and resilience.

The report identifies and name and address primal challenge, such as extenuate the wallop of innovative attack strategies like connivance and strategic fire, which can significantly thin out the effectiveness of IDS mechanics. By proposing a robust, voting - establish defense chemical mechanism, the generator offer a scalable solution to battle these sophisticated threats while maximizing the operational life-time of IoT system of rules. The SPN - establish analytical models show the effectualness of defense force strategies and offer a initiation for further research into more advanced fire - denial scenarios.

Furthermore, the authors propose the development of a real - world testbed, compose of 128 nomadic sensor nod, to formalize the proposed IDS design and assess its real - humankind performance. The testbed will serve as an essential step in bridge over the gap between theoretical mannikin and hardheaded deployment, providing empiric data point that will rectify the declare oneself defense scheme and ensure their applicability in substantial - world IoT environments.

In succeeding employment, the authors project to go the exemplar to cover even more complex attempt strategies and meliorate the scalability of the system to wield larger, more active networks. Through go forward research and real - world examination, the suggest IDS fabric let the potential to significantly enhance the security and reliableness of Autonomous Distributed IoT Systems, making them more live to come forth scourge and see to it their uphold functionality in mission - decisive applications.

Recommendation for Future Research:

1. **Advanced Attack Scenarios** : Succeeding research should explore more complex approach strategy, particularly **collusion - based attacks** and **strategical attacks**, where malicious client collaborate to corrupt the IDS or place specific vulnerability. This would help refine the IDS and ensure its effectiveness against coordinated scourge that are harder to detect. Further research could also examine insider threats in large detail, considering the behavior of compromise client that actively disrupt the system.
2. **Collusion - Aware Detection Mechanisms** : Given the challenges beat by connivance flak, it is vital to plan to a greater extent sophisticated **collusion - aware espial mechanisms**. This could demand enhance the voting - establish IDS by usher in anomaly detection and behavioral profiling to find unusual patterns indicative of coordinated malicious action. Research should sharpen on developing **fasten aggregation protocols** that resist manipulation by collude nodes.
3. **Improvement of SPN Models** : The current SPN mannikin can be further **refined** to include additional component such as adaptive flack strategies, **dynamic node behavior**, and the **evolving nature** of the network. Modeling should be expanded to incorporate the **resourcefulness constraints** of IoT knob and how these impact defense reaction strategies over time, as well as to simulate farsighted - term, continuous attacks that acquire in reaction to observe defenses.
4. **Existent - Time IDS Adaptation** : There is an opportunity to research **real - time adaptive IDS** system that can change detecting intervals (TIDS) and the number of ballot knob (m) based on system of rules stipulation or onslaught intensity level. This would help optimize the defense without overwhelming resourcefulness. Future study should concenter on developing automobile learning techniques for automatic modification of IDS parameter to respond dynamically to issue threat and changing environmental conditions.
5. **Energy Efficiency in IDS** : Collapse that **energy depletion** is one of the failure way in ADIoTS, it is important to concenter on energy - efficient IDS mechanisms that minimize the Energy Department expenditure of thickening while withal providing reliable violation detection. Research should investigate low - energy detection techniques that do not compromise the arrangement ’s power to observe and mitigate attacks.
6. **Scalability and Magnanimous - Scale Deployment** : While the current study focuses on 128 knob, future research should reach out this to great - exfoliation ADIoTS environments to valuate the scalability of the project IDS. Try Out on a network with thousands of nodes would allow for valuable perceptiveness into

the operation and limitations of the defense strategies. Investigate diffuse computing techniques for expectant - scale IDS operations may also help manage computational complexity.

7. **IoT Protocol - Specific Security** : Succeeding employment should view the specific exposure and demand of different IoT communicating protocols (such as MQTT, CoAP, or LWM2 M) and orient the IDS to deal protocol - specific approach vector. Integrating protocol - aware IDS into the defense framework will amend detection efficiency and accuracy.
8. **Integration of Blockchain for Security** : **Blockchain technology** can potentially enhance the security and integrity of the voting - based IDS by ply a decentralized, tamper - proof ledger for node behaviors and IDS votes. Research could investigate how blockchain - establish solutions could be integrated with the current IDS framework to enhance **trust** and prevent attacks like ballot stuffing or badmouthing.
9. **Cross - Layer Security Approaches** : Future research should research **cross - layer security department mechanisms** that combine physical, link, and application layers of the IoT network to provide more full-bodied defense chemical mechanism. By considering attacks that may span multiple layers, to a greater extent in effect countermeasure can be developed, tone the overall resilience of the ADIoTS.
10. **Empirical Testing and Validation** : As the paper aim the development of a testbed, future research should centre on formalise the models with genuine - world datum, experiment with a wide-cut stove of attack scenarios, and assessing the **impact of environmental factors** (such as meshwork rotational latency, bandwidth limitations, and node mobility) on the IDS 's effectiveness. Empirical testing can provide valuable brainwave into the **feasibleness and practicality** of deploying the advise IDS in real - Earth ADIoTS deployments.
11. **Multi - Tier IDS Framework** : Given the heterogenous nature of IoT networks, a **multi - tier IDS framework** that compound local detection at each client with **global analysis** of the system of rules could improve the overall security posture. Research could look into the synergism between local, edge - free-base, and cloud - establish IDS portion to declare oneself a scalable and flexible defense model.

References:

- Jin, S., & Liu, W. (2021). "A survey on intrusion detection techniques in Internet of Things." *Computer Networks, 190*, 107916.
- Sharma, A., & Sood, M. (2019). "Security challenges and solutions in the Internet of Things: A survey." *Computer Networks, 149*, 69-90.
- Han, Z., & Liu, Z. (2018). "Distributed Intrusion Detection System for the Internet of Things: A Review." *IEEE Access, 6*, 72709-72727.
- Baskiyar, G., & Sahoo, S. (2020). "Collaborative intrusion detection in the Internet of Things: A survey." *International Journal of Computer Applications, 975*, 0975-8887.
- Zhang, Z., & Zhang, H. (2020). "Modeling and analysis of intrusion detection system based on Stochastic Petri Nets in IoT networks." *Journal of Computer Networks and Communications, 2020*, 1-13.
- Zhao, Z., & Li, F. (2019). "A lightweight intrusion detection system for IoT-based on deep learning." *Future Generation Computer Systems, 97*, 46-56.
- Hassan, M., & Noura, H. (2021). "Energy-efficient intrusion detection for IoT systems: A review." *Computer Science Review, 40*, 100389.
- Al-Fuqaha, A., & Guizani, M. (2020). "Security and privacy in the Internet of Things: Challenges and solutions." *IEEE Transactions on Industrial Informatics, 16*(8), 5224-5232.
- Gao, W., & He, Q. (2017). "A survey of intrusion detection systems for Internet of Things: Applications, challenges, and future directions." *IEEE Transactions on Industrial Electronics, 64*(8), 6436-6446.
- Kim, T., & Choi, H. (2018). "A study on intrusion detection in distributed IoT systems: The role of collaborative security mechanisms." *International Journal of Computer Science and Network Security, 18*(6), 9-16.