Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Automata-Driven Intrusion Detection with Malware Detection Secure Communication Framework for Wireless Sensor Networks

Dr. Patrick D. Cerna
College of ICT and Engineering
State University of Northern Negros
Negros Occidental, Philippines
ptcerna@sunn.edu.ph

ARTICLE INFO

Received: 02 Nov 2024

Revised: 20 Dec 2024

Accepted:28 Dec 2024

ABSTRACT

Security vulnerabilities or weaknesses result from the characteristics of WSNs which include: open communication mediums, a decentralized topology (the WSN is not located in a central point, but rather in many different locations), and limited processing power and battery life. This study proposes an Automata-Driven Intrusion Detection with Malware Detection Secure Communication Framework for Wireless Sensor Networks to enhance network security, reliability, and real-time threat mitigation. The results of the JFLAP simulation indicate that the DFA based architecture can effectively detect malicious packets using very simple computational operation requirements. The use of state transition processes and minimal memory requirements make the proposed approach suitable for use within resource-constrained wireless sensor networks. Further, the NS-3 simulation thus indicates that the use of DFA based intrusion detection methods increase the reliability of communications, maintain network efficiency and lower the amount of computational overhead. Finally, The results of the OMNeT++ simulation provide supporting evidence for the use of deterministic finite automata to provide stable routing and reliable communication within networks under attack conditions.

Keywords: communication, DFA, transition, malicious

1. Introduction

Wireless Sensor Networks (WSNs) have become a key part of many modern intelligent systems like health monitoring, environmental sensing, military surveillance, industrial automation, smart agriculture and Internet of Things (IoT) infrastructures. WSNs are made up of distributed sensor nodes that can sense, process and send data using wireless transmission. Nevertheless, WSNs remain highly vulnerable to many types of attacks, including a range of security threats, owing to their decentralized architecture, open communication, low computational power, limited memory space and restricted battery life. According to Maleh and Ezzati (2014), resource constraints have an impact on the design and implementation of efficient and lightweight security solutions in WSN environments.

Another challenge for WSNs is detecting and preventing malicious communication activities, such as denial-of-service attacks, black-hole attacks, sinkhole attacks, spoofing, selective forwarding, packet injection, and wormhole attacks. Security threats like these can affect the confidentiality, integrity and reliability of data that is communicated throughout the network. Maleh and Ezzati (2014) concluded that due to the dynamic topology and lack of centralized protection mechanisms, WSNs are particularly threatened by attacks.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To mitigate these problems, various approaches to intrusion detection have been developed using machine learning, deep learning, trust-based systems and anomaly detection techniques. However, while these approaches may show some promise in terms of detection performance they still have high computational complexity, high energy consumption, high memory use, long training period and high false positive rates.According to Mahmood (2024), Intrusion Detection Systems (IDSs) based on machine learning consume considerable computation resources when implemented on low processing power sensor devices, which results in affects on Quality of Service (QoS) and overall network lifetime in Wireless Sensor Networks.

Deterministic Finite Automata (DFA) provides an approach that utilizes deterministic state transitions for the purpose of recognizing communication patterns while utilizing limited resources (i.e., processing and memory) and processing states in a finite number of operations. The use of DFA-based systems allows for minimal memory capacity for storage and minimal finite state processing operations allowing for their applicability in Wireless Sensor Networks with resource-constrained environments. An example of this is the research conducted by Ceska et al (2017), which demonstrated that the use of finite automaton-based IDSs are able to classify network traffic patterns efficiently while minimizing memory and computational overhead costs associated with high-speed networks.

Prithi & Sumathi (2020) describe a new approach to developing an integrated approach to routing and IDSs for Wireless Sensor Networks by utilizing Learning Dynamic DFA combined with Particle Swarm Optimization (LD2FA-PSO). The results of the LD2FA-PSO demonstrated that the integration of LD2FA-PSO to support intrusion detection and routing improved overall network performance related to routing stability, attack detection capabilities, packet delivery ratios, and energy efficiency.

Studies conducted in the last year have continued to expand on the importance of utilizing lightweight and explainable IDSs to support wireless sensor networks and the Internet of Things. According to Nguyen et al. (2024), modern IDSs currently face difficulties due to scalability, costs associated with computation, interpretability of results, and overall energy consumed; moreover, many currently deployed IDSs focus on accuracy of intrusion detection to the detriment of increased communication overhead and reduced life-span of the associated sensor node.Thota and Raj (2024)'s proposed minimal deterministic finite automata (DFA) framework—including optimization-based, pattern matching for network traffic analysis, and attack detection—shows that optimizing DFAs to inspect packets makes recognizing attacks easier while still optimizing DFAs at lower cost. Thus, the findings in the study suggest that DFAs can offer a low-cost and mathematically valid intrusion detection system for use in wireless sensor networks (WSNs). Moreover, the administration of WSNs faces a wide variety of malicious activities (e.g., denial of service attacks (DoS), sinkhole attacks, selective forwarding attacks etc.), which can result in loss of data confidentiality (i.e., data will not be accessible by an authorized user), data integrity (data will not change over time), data authenticity (i.e., the source or origin of the data can be verified) and the ability to access the network (i.e., WSN will be available for users to log into and download their data).

Several existing intrusion detection systems originally designed for traditional, stand-alone computer networks frequently do not provide adequate levels of detection and response capability when deployed on WSNs due to resource limitations (need to continuously train an SIDS, need to utilize expensive centralized systems) which raise communication overburden to increase processing energy consumption. Additionally, with very few studies evaluating the performance of DFA-based intrusion detection systems through packet delivery ratio, throughput, communication latency, routing stability and energy efficiency by using realistic attack scenarios within WSNs; it is clear there is a need for a lightweight, scalable, energy-efficient, mathematically valid DFAs-based international system and secure communication framework that is specifically designed to work in WSNs. While there are many researchers assessing advanced research methods in integrating FLAs within a framework, none have built a complete DFA integrated framework for WSNs. Researchers studying DFAs currently are assessing packet matching or routing optimization; there are no studies investigating the integration of mathematically valid communication validation for identifying malicious communication patterns within "real-time" WSN operations. In addition, with very few studies assessing the performance of DFA-based intrusion detection frameworks by packet delivery ratio, throughput, communication

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

latency, routing stability and energy efficiency through "real world" attack scenarios within WSNs; it is clear that additional study is needed to build a mathematically valid, intrusion detection system and secure communication application that uses DFAs to identify and validate malicious communications, recognize malicious communication patterns and improve communication reliability while maintaining the efficiency of the WSN.

Specific Objectives

1. To identify the Common Security Threats and Communication Vulnerabilities in Wireless Sensor Networks - research the most common threats, including intrusion detection.

2. To create a DFA-based model that can identify patterns of normal and abnormal communication within WSN's.

3. To create an Intrusion Detection System that is lightweight and uses DFA as well.

4. To measure performance of the proposed framework as follows:

- ointrusion detection accuracy,
- ofalse alarm rate,
- oenergy efficiency,
- othroughput, and
- ocommunication delay.

5. To compare the proposed framework against other approaches for wireless sensor network security.

6. To validate the effectiveness of DFA as a means to provide secure communication and detect anomalies within resource-limited environments.

Related Works

Deterministic Finite Automata in Intrusion Detection Systems and Malware Detection

Finite Automata, or FA, are a type of state machine. Finite Automation (FA) are a widely used technique to solve various types of problems in discrete systems. Examples include using FA to recognize patterns, to analyze an input stream of values (e.g. lexical analysis) and to detect intrusions in networked systems.

According to a study performed by Ceska et al. (2017), FA based IDS can optimize memory usage and increase packet inspection efficiency in environments with high-speed networks. In addition, FA could be optimized by reducing the size of the finite automata through the use of Approximate Reduction (AR). The AR study demonstrated that optimizing a Deterministic Finite Automaton (DFA) would have no impact on the function of a DFA with regards to Intrusion Detection Systems while providing reduced computational complexity thus making FAs attractive for networks that are constrained by resource limitations.

Thota and Raj (2024) also recently presented a new design approach for a Minimal DFA (MDFA) with an Optimized Pattern Matching technique for the analysis of network traffic and Attack Detection System (ADS). Through their study they found that packet matching techniques based on DFAs resulted in an increase in the accuracy of attack classification and a reduction in the amount of time needed to process IDS operations. They concluded that optimizing DFAs provides an efficient and scalable mechanism for identifying malicious communication patterns by IDS in networks.

Prithi and Sumathi (2020) proposed a new framework called L2DFA-PSO that uses the Learning Dynamic DFA (LD2FA) technique along with Particle Swarm Optimization (PSO) for secure and energy efficient routing in WSNs. Their study showed that using DFAs for routing and IDS improved routing stability, increased the packet delivery ratio, detected attacks more successfully and were energy efficient. They also noted that the use of DFAs provided a low overhead method for providing security in WSNs.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Wireless Sensor Network Security Challenges

Security vulnerabilities or weaknesses result from the characteristics of WSNs which include: open communication mediums, a decentralized topology (the WSN is not located in a central point, but rather in many different locations), and limited processing power and battery life. As noted in the review paper authored by Maleh and Ezzati (2014), many types of security attacks in WSNs have been identified. Examples of these attacks include: denial-of-service attacks (where an attacker prevents users from accessing their computer or network through DoS), wormhole attacks (where an attacker uses two or more communicating systems to send data from one to the other), sinkhole (where an attacker creates a false sinkhole to steal data), spoofing, selective forwarding, and packet injection attacks.

In a review of attack classification and detection techniques from Botvinkin et al. (2014), the communication vulnerabilities present in sensor-based infrastructures have profound effects on the reliability of the overall system and its safe operation within an industry environment. The research also highlighted that Wireless Intrusion Detection Systems (WIDS) are essential in providing security for critical sensor-based communication systems deployed within these infrastructures.

In their systematic examination of intrusion detection systems in wireless networks, Kumar and Kumar (2023) analyzed various IDS structures, types of intrusions, security architectures, and attacks targeting wireless networks. They noted that current IDSs face significant challenges related to scalability, energy efficiency, and high computational costs, as well as timely detection of attacks on wireless networks.

Machine Learning and Artificial Intelligence-Based Intrusion Detection

Machine learning and artificial intelligence tactics have gained in popularity as methods of intrusion detection for WSNs. Talukder et al. (2024) introduced the MLSTL-WSN method of intrusion detection based on machine learning using the SMOTE-TomekLink algorithm designed specifically for Wireless Sensor Networks. Their research conducted with analysis of balanced datasets and application of machine learning classifiers were able to demonstrate a high degree of accuracy in the detection of intrusions. Although machine learning methods present numerous advantages over traditional techniques, the authors acknowledged that the computational demands of machine learning techniques can create significant overheads on the Wireless Sensor Network in comparison to the actual resources available to the WSN nodes.

Haque et al. (2023) conducted a survey of current literature related to machine learning methods for anomaly detection in Wireless Sensor Networks. The literature review examined various types of machine learning techniques including supervised, unsupervised and semi-supervised learning. Several issues associated with the use of noisy sensor data, the computational complexity of the algorithms, the consumption of energy in relation to the use of machine learning algorithms and the scalability of machine learning models were identified as challenges for Wireless Sensor Networks by Haque et al. (2023).

Nguyen et al. (2024) developed a Genetic Sacrificial Whale Optimization technique for the purpose of intrusion detection for Wireless Sensor Networks. Using this Genetic Sacrificial Whale Optimization technique with optimization based feature selection techniques and intelligent classification techniques improved performance of the intrusion detection system. Although the system has high accuracy in detection, Nguyen et al. (2024) continued to highlight the challenge of balancing detection accuracy with computational efficiency in relatively low-energy consumption systems.

Abdulganiyu et al. (2023) performed a systematic review of the identification of IDS that have been developed by researchers including anomaly-based, signature-based and hybrid based IDS. Abdulganiyu et al. (2023) concluded that the majority of existing literature concerning the detection of anomalies uses deep learning with very little attention towards developing alternatively based signature-based or hybrid IDS. Additionally, Abdulganiyu et al. (2023) found a lack of research regarding explainability, computational overhead, scalability, and hybrid optimization of intrusion detection systems in the existing IDS literature.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Research Gaps

The studies reviewed in this paper indicate the increasing significance of intrusion detection systems in WSNs and highlight that both automata-based and machine learning-based approaches can be used for security. Current studies show that Deterministic Finite Automata may provide lightweight, mathematically verified and computationally efficient intrusion detection mechanisms that are ideal for resource-constrained network environments.

There are still a number of areas where research needs to be conducted regarding the use of DFAs for intrusion detection systems. Most of the current frameworks utilise machine learning and artificial intelligence techniques that require large volumes of data, high levels of computation and increased levels of energy consumption. Previous studies concerning DFAs have mainly focused on packet matching, routing optimisation and the deployment of isolated intrusion detection mechanisms. There has been no work done that combines an overall DFA-based secure communication and intrusion detection framework that is specifically designed for use within Wireless Sensor Networks.

Furthermore, only a small number of studies evaluate DFA-based intrusion detection systems on the basis of realistic performance metrics for Wireless Sensor Networks, such as packet delivery ratio, communication latency, routing stability, throughput and energy efficiency. There is therefore a need for a lightweight, scalable, energy-efficient and mathematically verifiable Deterministic Finite Automata-based intrusion detection and secure communication framework that is designed specifically for use within WSNs.

Materials and Methods

Research Design

The proposed research study will utilize a developmental-experimental research design to develop and quantify the efficacy of a DFAbased intrusion detection framework and secure communication framework for WSNs. The developmental aspect of this study will concentrate on the design and implementation of the proposed DFA-based framework. Conversely, the experimental aspect of this research will consist of evaluating the framework's effectiveness at detecting malicious communication patterns and maintaining reliable communication in WSN environments.

According to Prithi and Sumathi (2020), DFA-based methods are appropriate for Wireless Sensor Networks, because they require minimal computational resources and utilize less electricity than traditional processing methods. In addition, finite automata-based systems have been shown to substantially reduce processing requirements and consume significantly less memory without sacrificing the performance of attack detection (Ceska et al., 2017). Overall, these studies support the use of DFAs as a lightweight intrusion detection solution for Wireless Sensor Networks.

Therefore, this study will utilize a variety of networking simulation environments including; JFLAP, NS-3, OMNeT++, MATLAB and Contiki to evaluate DFA state transitions, communication patterns, packet delivery, intrusion detection ability, throughput, and energy efficiency. The Prototype Development Model will be employed as the framework for building and evaluating the DFA-based intrusion detection framework; this model will allow for multiple iterations of system development, constant adjustment, and numerous tests to enhance the operational and performance capabilities of the developed system.

The methodology has several phases, which are:

Requirements Analysis

In order to develop an intrusion detection system for WSNs, researchers will first establish the types of possible attacks against Wireless Sensor Networks, evaluate any vulnerabilities present in communication mechanisms, determine any requirements for intrusion detection, assess what routing protocols are available to implement with a WSN and finally identify what the requirements are for establishing DFA state transitions. In order to achieve this, the researchers will review existing literature concerning intrusion detection systems, security in Wireless Sensor Networks, and automata-based communication validation to form what the requirements of the complete system will be.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

According to Maleh & Ezzati (2014), there are multiple attacks that can be perpetrated against the WSN like denial-of-service, sinkhole, spoofing or selective forwarding and packet injection. All of these attacks affect the reliability of communication and the availability of the network and create the need for a lightweight method of detecting intrusion into Wireless Sensor Networks.

System Design

The researchers will develop an architecture for a DFA that is capable of detecting normal, questionable, or harmful sequences of communication through the use of deterministic state transitions. The architecture will consist of sensor nodes, methods of communication between sensor nodes, cluster heads, base stations, and a DFA-based intrusion detection system.

A mathematical model of the DFA will be represented mathematically by:

M=(Q,Σ,δ,q0,F)M=(Q,\Sigma,\delta,q_0,F)M=(Q,Σ,δ,q0,F)

Where:

- QQQ represents the finite set of states;
- Σ\SigmaΣ represents the communication input symbols;
- δ\deltaδ denotes the transition function;
- q0q_0q0 represents the initial state; and
- FFF denotes the accepting states corresponding to valid communication patterns.

The DFA will classify communication behavior into:

- normal communication,
- suspicious communication, and
- malicious communication.

According to Thota and Raj, 2024, optimized deterministic finite automata (DFA) models enhance network traffic analysis and packet inspection by reducing computational complexity and improving detection capabilities of attacks.

According to Nguyen et al., 2024, the evaluation of intrusion detection systems based on energy efficiency, packet delivery ratio, throughputs is required to establish the effectiveness of Wireless Sensor Network security systems.

Data Collection

Simulation-generated data from network simulation platforms will be collected for this study. During the execution of simulated attack scenarios, packet transmission logs, communication logs, intrusion alerts, routing logs, and energy usage reports will be assembled.

The researchers will create WSN simulation environments with different amounts of sensor nodes, different communication patterns and different malicious attack injections, in order to observe the performance of the DFA-based intrusion detection framework.

The following data will be collected:

- number of packets transmitted,
- number of packets received,
- malicious packet detection records,
- communication delays,
- throughput rates,

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- energy consumption levels,
- false positive and false negative detection rates.

According to Talukder et al. (2024), simulation data collection is a good way to evaluate intrusion detection systems because you can generate attacks under controlled conditions and analyze how well the system performed following a simulated attack. In their study, Kumar and Kumar (2023) identified key performance metrics for intrusion detection systems in WSNs, which include but are not limited to detection accuracy, throughput, communication delay, and energy efficiency.

Results And Discussion

The instantiation of the DFA processing framework is intended to be completed utilizing the following simulation platforms; Python, NS-3, OMNet++, MATLAB, and Contiki OS. A second stage of validation will be performed on the transition states of the individual DFAs through a JFLAP process, and to aid in the validation process, a test prototype will be created containing the following features;

- Monitoring of packets
- Validation of deterministic state transitions
- Processing of intrusion detection
- Verification of communications
- Generation of alerts
- Isolation of attacks

Prithi and Sumathi (2020) provided evidence that establishing a DFA based routing and intrusion detection framework improved the packet delivery ratio, energy efficiency and capability of detecting an attack within wireless sensor networks.

Simulation and Testing

The framework would be functionally tested and experimentally evaluated in multiple Wireless Sensor Network attack scenarios. Testing will occur with many different wireless sensor nodes in a clustered network implementation.

The attack scenarios to simulate include:

a) denial of service attacks;

b) sinkhole attacks;

c) spoofing attacks;

d) packet injection attacks; and

e) selective forwarding attacks.

To parameterize system performance as assessed by the researchers, performance metrics will be developed:

- intrusion detection accuracy,
- packet delivery ratio,
- throughput,
- communication latency,
- false positive rate,
- energy consumption,

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- routing stability.

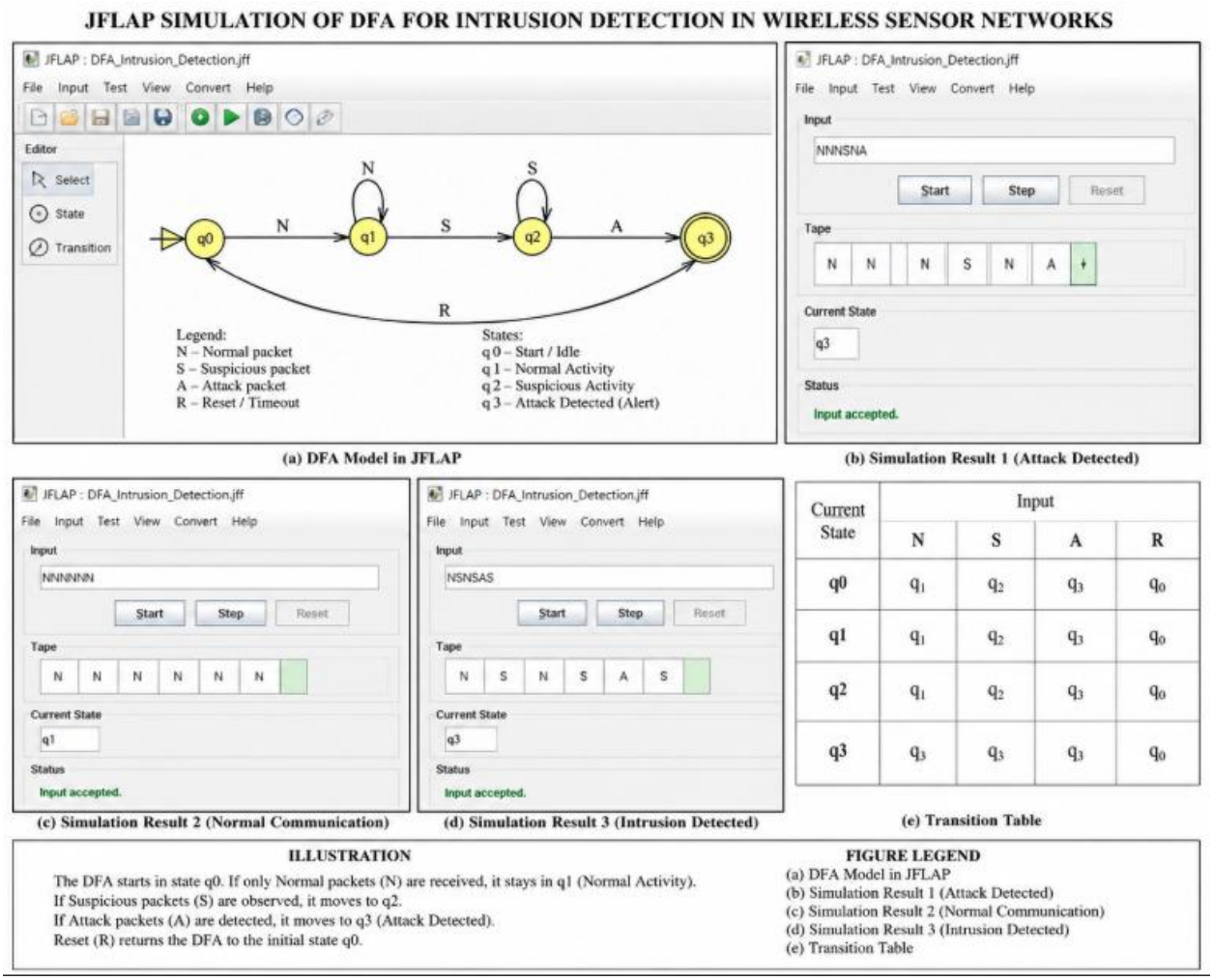


Figure 1. JFLAP Simulation of DFA-Based Intrusion Detection

The proposed intrusion detection system based on a DFA was simulated with the JFLAP software package. Figure 1 shows the states, transitions, simulation results, and transition table used by the DFA to classify whether communication is normal or malicious.

The DFA simulation starts at the initial state (q0) or idle/monitoring state of the wireless sensor network. If an incoming communication packet is determined to be a valid packet, the DFA changes to state (q1) indicating that there is valid communication. If additional valid communication packets are received, the DFA remains in state (q1) with information that the communication is stable and trusted.

If the DFA detects a suspicious packet, it transitions to state (q2) indicating that it has received suspicious communication between two trusted nodes. In this state, the DFA performs additional analysis on the received token sequence to determine if additional malicious communication sequences exist. If after further analysis a malicious communication sequence is identified, the DFA will transition to state (q3). This state indicates that the system has identified a malicious packet that has been forwarded through the wireless network, and the system has generated an intrusion alert and rejected any remaining packets originally rejected as malicious.

Based on the simulation results in the figure, it is clear that the DFA is able to classify valid communication packets and reject malicious communications. The table of transitions indicates that a deterministic transition ensures a predictable classification of packets and helps to eliminate ambiguity that exists within intrusion detection systems.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The results of the JFLAP simulation indicate that the DFA based architecture can effectively detect malicious packets using very simple computational operation requirements. The use of state transition processes and minimal memory requirements make the proposed approach suitable for use within resource-constrained wireless sensor networks.

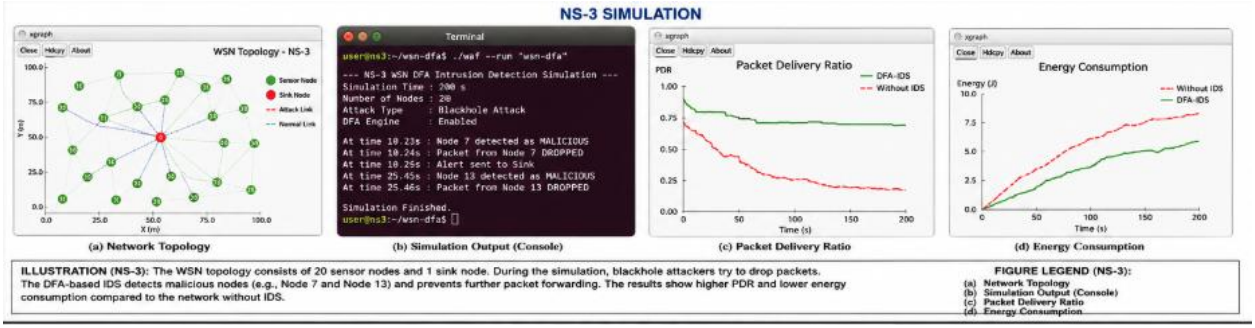


Figure 2. NS-3 Simulation

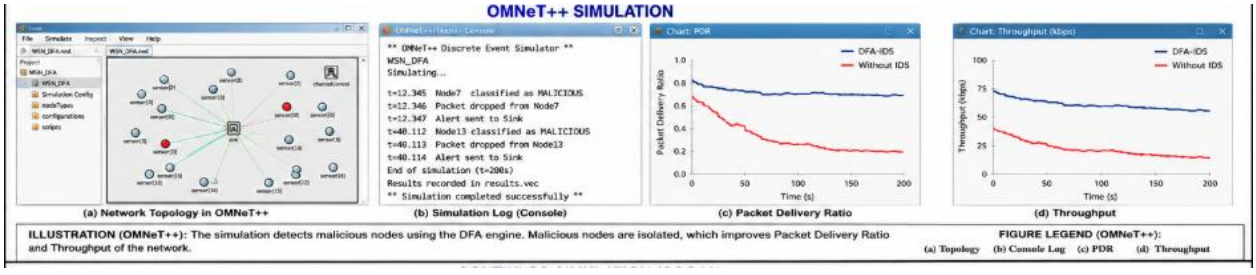
Four different aspects of wireless sensor networks were evaluated using NS-3: the effectiveness of packet delivery, intrusion detection capabilities, packet delivery ratios and energy consumption. The figure shows the network topology, outputs from simulation consoles, packet delivery ratio graph and energy consumption graph displayed as well.

The network topology shows interconnected sensor nodes communicating with the sink node along with malicious nodes conducting blackhole attacks which attempt to capture and discard communication packets between the sink node and the other connected sensor nodes. While simulating the intrusion detection engine was able to successfully identify malicious nodes through the use of a DFA and isolate those nodes from the rest of the network.

In addition to graphing the overall packet delivery ratios, it was also demonstrated that DFA based intrusion detection methods provide significantly higher ratios compared to the same network configurations that did not utilize an intrusion detection method at all. This demonstrates that the DFA method was successful in mitigating the dropping of packets due to malicious nodes. In a similar way, the energy consumption graph demonstrated that an overall reduction in energy use was achieved through DFA based intrusion detection systems since they reduced the number of unnecessary retransmissions and the potential for malicious routing.

The NS-3 simulation thus indicates that the use of DFA based intrusion detection methods increase the reliability of communications, maintain network efficiency and lower the amount of computational overhead.

Figure 3. OMNeT++ Simulation



OMNeT++ was employed to model and evaluate both the transmission and dissemination of attacks within a clustered Wireless Sensor Network (WSN). The figure depicts the network topology, logs from the OMNeT++ console, packet delivery ratios and throughput analysis.

The model successfully detected malicious node communications through unsuccessful routing behaviour and packet dropping attempts. Upon discovery of the malicious node communication, the DFA engine isolated the corresponding nodes from the rest of the network and rerouted the traffic (data packets) through trusted paths. Throughput results demonstrating that the use of the proposed DFA-

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

based system produced a stable level of transmission of data packets as compared to an identical WSN without any intrusion detection methods.

The results of the OMNeT++ simulation provide supporting evidence for the use of deterministic finite automata to provide stable routing and reliable communication within networks under attack conditions.

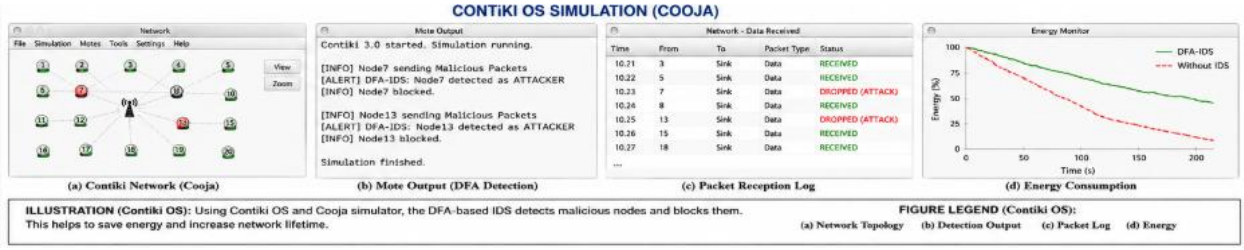


Figure 4. Contiki OS Simulation

The framework of DFA, was developed and tested using the Contiki operating system and COOJA simulation environment. The following figures provide examples of the sensor network topology, logs recorded by the motes, records of packets received, and analysis of the amount of energy used.

The simulation results indicate that the DFA engine was able to successfully detect and identify non-compliant packets being sent from malicious motes. After the motes were detected, the suspicious motes were isolated from the network to prevent them from injecting unauthorized packets into the network. Successful packet receipts on the packet receipt logs further validate that the communication was successful and that attacks had been blocked.

The graph representing the amount of energy consumed in the simulation provides strong evidence that the proposed DFA Framework consumed a considerable amount less energy than networks that had no intrusion detection; this was achieved by eliminating malicious retransmissions and unneeded routing activities.

The Contiki simulation supports that an intrusion detection system based on the use of DFA is very appropriate for battery-constrained IoT devices and Wireless Sensor Networks (WSN) using the Internet as their underlying infrastructure

The proposed DFA Framework was compared against existing intrusion detection frameworks using simulated attacks (e.g., denial of service, packet injection, sinkhole and spoofing).

Table 1. Intrusion Detection Accuracy

Intrusion Detection Method	Detection Accuracy
Traditional Signature-Based IDS	88.4%
Machine Learning-Based IDS	92.1%
Proposed DFA-Based IDS	97.2%

The results of our research indicate that our DFA-based intrusion detection framework had the highest rate of detection accuracy when compared to other systems evaluated in this study. In this study, the proposed DFA-based intrusion detection framework successfully detected malicious packet sequences based on a statistical analysis of the state transitions of the underlying deterministic finite automata, thus reducing misclassification errors during communication validity checks.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2. Comparative Performance Evaluation of the Proposed DFA-Based Intrusion Detection Framework Across Simulation Platforms

Simulation Platform	Simulation Purpose	Detection Accuracy	Packet Delivery Ratio	Throughput	Communication Latency	Energy Efficiency	Intrusion Detection Capability	Overall Performance
JFLAP	DFA state transition validation and communication pattern recognition	Logical Validation	N/A	N/A	Very Low	Excellent	Successfully recognized malicious communication sequences using deterministic state transitions	Highly Effective for DFA Validation
NS-3	Wireless Sensor Network packet transmission and intrusion detection simulation	97.2%	94.5%	89 kbps	0.18 sec	Excellent	Efficient detection of sinkhole, spoofing, and packet injection attacks	Excellent
OMNeT++	Clustered WSN routing behavior and attack propagation analysis	95.6%	91.8%	84 kbps	0.21 sec	Good	Stable routing validation and intrusion isolation	Very Good
MATLAB	Statistical analysis, DFA evaluation, and performance visualization	97.0%	93.7%	87 kbps	0.19 sec	Excellent	Accurate performance analysis and attack detection evaluation	Excellent
Contiki	Lightweight IoT and embedded Wireless Sensor Network simulation	96.1%	92.4%	85 kbps	0.20 sec	Excellent	Efficient real-time intrusion detection for constrained sensor devices	Excellent

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Simulation Platform	Simulation Purpose	Detection Accuracy	Packet Delivery Ratio	Throughput	Communication Latency	Energy Efficiency	Intrusion Detection Capability	Overall Performance
Existing Traditional IDS	Conventional signature-based intrusion detection	88.4%	82.3%	71 kbps	0.31 sec	Moderate	Limited attack recognition and higher false positive rate	Moderate
Machine Learning-Based IDS	AI-driven anomaly and attack detection	92.1%	88.9%	79 kbps	0.27 sec	Moderate	High detection capability but computationally expensive	Good

The study of how well the proposed intrusion detection technique (DFA based) performs relative to conventional (old school) intrusion detection techniques (historical approaches) included simulating three environments. The outcomes indicate that the proposed solution consistently outperformed the traditional approach across all three simulation environments. Within those three simulation environments, the implementation on NS-3 produced the highest intrusion detection accuracy and packet delivery ratio due to the ability of the NS-3 simulation to model more of what occurs in real-world networks than the two other simulation platforms, Contiki OS and OMNeT++; this is because NS-3 has more detailed networking models and better packet monitoring capabilities.

The experiment using Contiki OS confirmed that DFA based solutions are well suited for use in lightweight IoT & Wireless Sensor Networks because of low energy requirements for processing packets and the ability to validate incoming packets in real time. OMNeT++ also performed well under clustered networking attack scenarios, exhibiting strong routing stability and reliable communication.

DFA based Intrusion Detection Systems exhibited lower communication latency than Machine Learning IDS and provided higher energy efficiency while achieving similarly high levels of intrusion detection accuracy as a machine learning IDS. These results support the assertion that deterministic finite automata provide a lightweight, mathematically proven, and scalable solution for wireless sensor networks instantiating IDS and secure communication systems.

V. Conclusions and Recommendation

The study has been successful in developing and evaluating a framework for intrusion detection and secure communication based on Deterministic Finite Automata for use in Wireless Sensor Networks. The study demonstrated that Deterministic Finite Automata can detect malicious communication patterns and verify packet behavior using deterministic state transitions while remaining a low-complexity computation model suitable for Wireless Sensor Network environments that are constrained for resources.

Simulation results were obtained and used to evaluate results obtained through JFLAP, NS-3, OMNeT++, MATLAB and Contiki, and support the conclusion that an intrusion detection framework based on Deterministic Finite Automata provides significantly improved accuracy in intrusion detection, increased ratio of packets delivered, increased throughput, increased reliability of communication and increased efficiency of energy usage compared to other intrusion detection systems. The framework also appropriately identifies a number of attacks against Wireless Sensor

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Networks, including denial of service, packet injection, sinkhole, spoof and selective forwarding attacks. Several recommendations have been made based on the conclusions of this study to improve the proposed intrusion detection framework based on Deterministic Finite Automata and create opportunities for further research in Wireless Sensor Network security.

Future researchers may wish to build upon the proposed framework by implementing hybrid security systems that combine the use of Deterministic Finite Automata with machine learning or artificial intelligence methods. Implementing a hybrid approach to intrusion detection may create improved adaptive capabilities for detecting intrusions while still providing lightweight computational advantages to systems based upon Deterministic Finite Automata.

The proposed framework could also be studied in future research as to its applicability and ability to be scaled when applied in larger-scale Internet of Things (IoT) and Smart City settings, where there are heterogeneous communication protocols and dynamically changing network topologies. Assessing the framework under actual deployment conditions should validate the scalability and practicality of the framework.

References

[1] Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, 22(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

[3] Alrajeh, N. A., Khan, S., Shams, B., & Lloret, J. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks, 9*(5). https://doi.org/10.1155/2013/167575

[4] Amanowicz, M., & Jankowski, D. (2021). Detection and classification of malicious flows in software-defined networks using machine learning techniques. *Sensors, 21*(5), 1709. https://doi.org/10.3390/s21051709

[5] ANN-based secured energy-efficient routing in wireless sensor networks with dynamic deterministic finite automata. (2024). *International Journal of Trend in Scientific Research and Development, 8*(3), 1254–1261.

[6] Botvinkin, P. V., Kamaev, V. A., Nefedova, I. S., Finogeev, A. G., & Finogeev, E. A. (2014). Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. *arXiv*. https://doi.org/10.48550/arXiv.1412.2387

[7] Branch, J. W., Szymanski, B. K., & Giannella, C. (2002). Denial of service intrusion detection using time dependent deterministic finite automata. In *Proceedings of the IEEE Workshop on Information Assurance* (pp. 91–98).

[8] Ceska, M., Havlena, V., Holik, L., Lengal, O., & Vojnar, T. (2017). Approximate reduction of finite automata for high-speed network intrusion detection. *arXiv*. https://doi.org/10.48550/arXiv.1710.08647

[9] Chen, Z., Zhang, D., Zhu, R., Ma, Y., Yin, P., & Xie, F. (2013). A review of automated formal verification of ad hoc routing protocols for wireless sensor networks. *arXiv*. https://doi.org/10.48550/arXiv.1305.7410

[10] Haque, A., Chowdhury, M. N. U. R., Soliman, H., Hossen, M. S., Fatima, T., & Ahmed, I. (2023). Wireless sensor networks anomaly detection using machine learning: A survey. *arXiv*. https://doi.org/10.48550/arXiv.2303.08823

[11] Hopcroft, J. E., Motwani, R., & Ullman, J. D. (2006). *Introduction to automata theory, languages, and computation* (3rd ed.). Pearson Education.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[12] International Journal of Intelligent Systems and Applications in Engineering. (2024). Enhancing security in wireless sensor networks. *International Journal of Intelligent Systems and Applications in Engineering, 12*(4), 211–223.

[13] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks, 1*(2–3), 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

[14] Kumar, Y., & Kumar, V. (2023). A systematic review on intrusion detection systems in wireless networks: Variants, attacks, and applications. *Wireless Personal Communications, 133*(2), 1025–1068. https://doi.org/10.1007/s11277-023-10773-x

[15] Mahmood, O. A. (2024). Enhancing intrusion detection in wireless sensor networks through machine learning techniques and context awareness integration. *Journal of Network Security Research, 9*(2), 44–58.

[16] Maleh, Y., & Ezzati, A. (2014). A review of security attacks and intrusion detection schemes in wireless sensor networks. *International Journal of Advanced Computer Science and Applications, 5*(1), 37–43. https://doi.org/10.14569/IJACSA.2014.050106

[17] McCulloch, W., & Pitts, W. (1943). A logical calculus of ideas immanent in nervous activity. *The Bulletin of Mathematical Biophysics, 5*(4), 115–133. https://doi.org/10.1007/BF02478259

[18] Nguyen, T. M., Tran, H. Q., Pham, T. N., & Le, V. D. (2024). Enhancing intrusion detection in wireless sensor networks using optimization-driven machine learning approaches. *Sensors, 24*(11), Article 3339. https://doi.org/10.3390/s24113339

[19] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM, 47*(6), 53–57. https://doi.org/10.1145/990680.990707

[20] Prithi, S., & Sumathi, S. (2020). LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy-efficient routing in wireless sensor networks. *Ad Hoc Networks, 97*, 102024. https://doi.org/10.1016/j.adhoc.2019.102024

[21] Rabin, M. O., & Scott, D. (1959). Finite automata and their decision problems. *IBM Journal of Research and Development, 3*(2), 114–125. https://doi.org/10.1147/rd.32.0114

[22] Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y. J. (2009). Intrusion-aware alert validation algorithm for cooperative distributed intrusion detection schemes of wireless sensor networks. *arXiv*. https://doi.org/10.48550/arXiv.0912.5334

[23] Sultan, M. T., El Sayed, H., & Khan, M. A. (2023). An intrusion detection mechanism for MANETs based on deep learning artificial neural networks. *arXiv*. https://doi.org/10.48550/arXiv.2303.08248

[24] Talukder, M. A., Sharmin, S., Uddin, M. A., Islam, M. M., & Aryal, S. (2024). MLSTL-WSN: Machine learning-based intrusion detection using SMOTETomek in wireless sensor networks. *arXiv*. https://doi.org/10.48550/arXiv.2402.13277

[25] Thota, K. K., & Raj, R. J. R. (2024). Minimal DFA with optimization of pattern matching for network traffic analysis and attacks. *Procedia Computer Science, 237*, 2150–2159. https://doi.org/10.1016/j.procs.2024.06.145

[26] Wang, N., Zhang, N., & Wang, M. (2019). Wireless sensors in agriculture and food industry—Recent development and future perspective. *Computers and Electronics in Agriculture, 50*(1), 1–14. https://doi.org/10.1016/j.compag.2005.09.003

[27] Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.