Ngr. J. Multi. vol-2, issue-1 (Jan-2026) pp-37-48

ISSN: 3108-2750(Online)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Review Article

Information Theory and Its Role in Cyber Security - Status and Future Trends

Dr. Eng. Prof. Sattar B. Sadkhan [1], Dhilal M. Reda[2]

[1,2] *University of Babylon, IT college, Hilla, Iraq*

ABSTRACT:

The paper examines the role and importance of information theory in the field of cybersecurity. More than 26 research papers related to the use of information theory in cybersecurity were collected. This paper specifically addresses the areas in which information theory has been used, as well as the important roles it plays in cybersecurity. The role of information theory has varied from detecting and classifying cyberattacks to developing routing algorithms, image encryption, and systems analysis.

Keywords: *cyber, security, information theory, entropy, attacks.*

INTRODUCTION

This research paper collects 26 research papers from 2020-2025. This includes the use of information theory in the field of cybersecurity. Cybersecurity encompasses the protection of any digital asset connected to the World Wide Web. This may include protecting computers, mobile devices, the Internet of Things (IoT), cloud services, and networks. Network security involves detecting and preventing threats from various types of potential attacks. This includes protecting networks like ISDN-based SDN from DDoS attacks, safeguarding industrial and commercial processes connected to the internet, such as IoT-based SDN, protecting physical systems connected to the network, such as communication-based train control systems, and securing data transmission in IoT over wireless networks.

The structure of this paper is presented with the introduction in Section I and the literature review in Section II. The uses of information theory in various fields, as well as forms of using information theory, are mentioned in Section III. The results are in Section IV, and the conclusion is in Section V.

LITERATURE REVIEW

This research paper collects the research papers from 2020-2025. This includes the use of information theory in the field of cybersecurity. Researchers in [1] have proposed a volumetric DDOS detection scheme for IOT networks. This scheme consists of three stages: a traffic preprocessor, an entropy calculator, and a detection and alarm module. The traffic processor monitors the SDN environment to get traffic packets in real-time, then extracts traditional RFC (5-tuples) appended with the time stamp of each packet. Also single-directional packet filter is used to realise early detection. In the entropy calculator, a sliding time window is used to speed up entropy calculation, which reduces the time complexity from O(n) to O (1). Joint entropy of the timestamp attached to 5-tuples of source and destination packets is computed in one of the methods: (variation updating method) or (value counter dictionary and counter matrix). In the detection and alarm module, a quintile deviation check algorithm is proposed, which takes the preprocessed and real-time joint entropy to make an immediate check and alarm for suspicious packets. Results have shown that this algorithm provides low latency and accurate performance.

Researchers in [2] have addressed spoofing attacks on Wi-Fi-based GPS systems. They have addressed two possible attacks on GPS systems: location spoofing and privacy attacks. A Defence scheme is proposed. The basic idea of the defence scheme is to reproduce the base stations **(BS)** ' tags

Corresponding author: Dr. Eng. Prof. Sattar B. Sadkhan

DOI: 10.5281/zenodo.18642252

Received: 15 Jan 2026; **Accepted:** 29 Jan 2026; **Published:** 30 Jan 2026

of the neighbouring base stations based on time and location. The defence scheme relies on a witness (not a user) to generate BS tags for the neighbouring base stations and transmit them to the server. The BS tag generation process involves several steps, including extracting location-related parameters from the BS signal, using entropy from information theory to select an unpredictable frame (high entropy) which has strong resistance to location spoofing attacks, and finally using a bloom filter with some hash functions to obtain a fixed BS tag length and reduce the system storage capacity.

The researchers have presented in [3] a traffic anomaly detection algorithm based on Intuitionistic Fuzzy Time Series (IFTS) graph mining. First, capturing traffic data over a series of time intervals (1..t). This data contains packet attributes. Second, the entropy of these attributes, which represent random events, is calculated. These entropy values represent the vertices of the graph; the edge weights of the graph reflect the similarity of the changes in entropy of two vertices connected by the edge; the larger the weight, the more similar the changes. Third, an IFTS forecasting model is used to predict the entropy values of these random events for time (t+1). Fourth, an IFTS graph for period (1..t) is constructed, and based on this, the IFTS graph for time (t+1) is predicted. Fifth, the support degree is calculated for each subgraph, and thus, the subgraph is mined. Sixth, a frequent subgraph is calculated to generate anomaly vectors. Seventh, the distance between anomaly vectors is calculated. Finally, an autoregressive model is used to identify an anomaly.

Researchers in [4] investigated the impact of DDOS attacks on the Software Defined Network (SDN) controller, in an Integrated Space-Terrestrial Network (ISDN). This work focuses on nodes' evaluation in the routing paths. They built a trusted routing matrix (TRM), which consists of the trusted models for all routing nodes. The trusted model of a single routing node is built based on the comprehensive entropy estimation of all characteristics. Then they proposed two routing models: first, trusted Routing (TR) based on TRM and second, hybrid routing (HR) models based on TRM and traditional QoS parameters, for evaluating trusted paths. Results showed that the proposed algorithm can avoid network traffic attacks and can ensure security to a large extent.

Researchers in [5] have suggested a malware entropy sequence reflective family (MESRF) method for classifying malicious programs by entropy and wavelet decomposition. This method relies on the extraction of global and local features, and it can be summarised as follows: at first, the training data represented by malware is collected, and then raw data is extracted from the malicious program. After that, raw bytes are divided into blocks, and all blocks are 256. Calculate the entropy of each block and get a vector that represents the malware's entropy sequences. To find general features, general features are extracted from the entropy vector. To find local features. Entropy sequences go through two stages: extraction and vectorisation. The proposed method achieved 99.83% accuracy and good detection speed for the malware in malimg database.

Researchers in [6] have proposed a scheme to detect Sybil DDOS attacks in the Internet of Vehicles. The scheme goes through three main stages: traffic processor, entropy calculator and detection module. The principle of entropy from information theory is used to analyse the data distribution, and in order to speed up the calculation of the entropy value, two principles were used: sliding calculation and incremental calculation. In order to identify and diagnose the attack, the Fast quartile deviation check (FQDC) algorithm was proposed. The evaluation results showed that the algorithm successfully detected all attacks in the F2MD database, and it has an average alarm delay of 4.9193 seconds and an average temporal false omission rate of 1.6024%.

The researcher in [7] has developed an entropy-defined direct batch growing hierarchical self-organising mapping (ED-DBGHSOM) method for detecting anomaly networks. In this paper, we develop a previously established classical model, DBGSOM, using entropy instead of cumulative error to determine whether a network is growing. Entropy is used to represent the purity of a dataset. A new concept of entropy, resembling entropy element (REP), is also proposed to calculate the probability of an element occurring within a data vector. REP provides a more accurate classification of natural

data vectors and attacks after data clustering processes. The advantage of this model is that it is dynamically adaptable and can change with changing datasets. The results of the proposed method show that the detection rate and false positive rate are superior when compared with previous works.

Researchers in [8] have proposed a method for encoding multiple images based on a 3D chaotic map and a substitution box. The proposed method goes through four stages: merging images into a single image by merging their colour channels, permuting the colour channels of the merged image using a 3D chaotic map technique, constructing a substitution box based on the AES substitution box, and permuting the alternative RGB channels using a substitution box. To determine the security and strength of the proposed method, a set of analysis methods was relied upon. Regarding information theory, entropy has been used to measure the degree of randomness of an encryption method. In a normal image, randomness is 8, but after using the encryption method, it was close to 8 , which indicates the strength of the encryption method.

Researchers in [9] have proposed three methods that contribute to detecting malware. These methods are considered an effective first step before applying machine learning algorithms. The first method: 2D-histogram entropy map, which is based on entropy information and a fixed size. The second method: histogram entropy visualisation. This method identifies key patterns of malware. It uses the output of the first method (fixed 2D entropy feature), analyses it, and visually reconstructs it. The third method: prototype selection algorithm. This method relies on constructing a hyperrectangle which divides the input space into smaller regions, and each region contains some instances within the same class. This method generates a small dataset containing meaningful instances from the original dataset. The goal of training a machine learning algorithm on small datasets containing meaningful instances will reduce training time and save storage space. The results showed that classification performance reached 98% or more using histogram feature entropy. The results also showed that using a prototype selection algorithm reduces the dataset size by 50%.

Researchers in [10] have proposed a security framework for the industrial internet of things (IIOT) based on software-defined network (SDN). This framework is based on information theory and blockchain and is implemented in two stages using an intra-domain mitigation scheme and an inter-domain mitigation scheme. Intra-domain can be explained as follows: eight features are selected. These features are arranged in pairs for each packet, and the mutual information for each pair is calculated. These values are accumulated and stored in a set. The joint entropy of the values in the first matrix is calculated, and the conditional entropy of the values in the second matrix is calculated. If an attack is found, the controller will send a new flow table rule to the switch to exclude the illegal IP address and ensure that this rule has the highest precedence for execution by the switch. As for the second stage, inter-domain, (shortly: detected attacks in the intra-domain scheme are uploaded to a smart contract on the blockchain to block these attacks). The results have shown that this framework is more effective in detecting low-rate attacks than existing attack detection methods that use joint entropy or conditional entropy alone, and that it is also more effective than others in detecting high-rate attacks when combined with a smart contract.

Researchers in [11] have proposed a DEMI application to detect and mitigate DOS attacks on SDN. This application DEMI goes through four stages: detection, mitigation, heavy load and system management. In the detection stage, a certain number of invalid requests are collected within a specific window time and features. The entropy value is calculated for the extracted destination IP address within a time window. If the value is low, it indicates that the packets are centred around a specific IP destination address, and it is an indicator of an attack. The Entropy value is compared with an adaptive threshold mechanism based on an exponentially weighted moving average (EWMA). The researchers obtained amazing results. For example, in the attack scenario, the number of exchanged control packets is almost similar to the no-attack scenario.

Researchers in [12] have presented a new approach to detecting malicious nodes in an ad hoc network. This approach relies on a combination of cluster-based entropy and machine learning. It can be

summarised as follows: first, the network is divided using the LEACH protocol. It divides the network into clusters. For each cluster, the head is randomly selected and changes periodically. Next, a trust value is calculated for each node, including the header. The trust value is calculated for each node based on its behavior in passing the packets. This trust value is used to calculate the trust entropy. The calculated entropy value for each node is then compared to a threshold. If the entropy value is greater than the threshold, the node is then considered trusted; otherwise, it is considered malicious and is detected and blocked. The geographic routing algorithm is applied as follows: if a node in one of the clusters wants to send data to the base station (BS), it will choose the node with the highest entropy and closest to the cluster head (CH) to deliver the data to it. The new dataset generated from a simulation of attack detection in an ad-hoc network-based trust entropy is used to train the proposed classification algorithm. The proposed method achieved 35% higher DPR and 23% higher throughput when compared with TASEE-HP-MANET, TSA-DIRA-MANET, and TAID-5G-MANET methods.

Researchers in [13] have addressed the security of MANET. It lacks a central control centre and is therefore vulnerable to malicious attacks. Researchers proposed a new cloud fuzzy Petri net (CFPN)-based reasoning mechanism. It passes in four stages: first, cloud-based fuzzy production rules CFPRs, Second, cloud-based rule representation for MANET, Third, calculation of truth degrees of condition propositions. Then they proposed a trust entropy routing algorithm to compute the entropy of a path. The path with the smallest entropy was the highest trust value and will be added to the routing table. A researcher employed CFPN and established the TUE-OLSR routing protocol based on the OLSR routing protocol. Results showed that the proposed protocol is better than the FPN-OLSR and OLSR protocols in terms of packet delivery ratio and average delay.

Researchers in [14] have addressed the issue of secure pairing of mobile devices in multimodal transportation (train, car, tram) using accelerometer data. They suggested the encrypted key exchange Diffie-Hellman (EKE-DH) protocol. This protocol ensures secure communication between mobile devices using accelerometer data. This data is provided in Cartesian form and goes through several stages: Temporal Synchronisation, Collect Data, Signal processing and byte extraction. In byte extraction, the data is divided into a set of windows ready for the key exchange stage in the EKE-DH protocol. Before using accelerometer data in the proposed protocol, the security of the data is analysed using the hamming distance, which must be zero and entropy. When the entropy value of the accelerometer data is low, this data is easy to predict and is not suitable as a secret key for the protocol, and vice versa.

Researchers have proposed in [15] an awareness model using singular value decomposition (SVD) and gated recurrent unit (GRU) with progressive residuals detecting (PRD) algorithms to enhance the operation of communication-based train control (CBTC) systems. The proposed model used the entropy from information theory in the SVD algorithm to select the dimensions that retain the most information and exclude other less important dimensions in the physical and network layers. These dimensions are then fed into a GRU neural network with an ORD algorithm to learn relevant data from the physical layer, predict situations, and trigger alerts in case of danger.

Researchers in [16] proposed novel solutions for three hijacking attacks targeting the SDN topology. For the first attack, the researchers proposed two solutions: verifying the legitimacy of host migrations based on two conditions. The first condition is maintaining a host mapping table. The second condition is ensuring the source of an LLDP frame. Regarding the second attack, the forgery link fabrication attack, the researchers set two conditions for a solution. The first condition ensures the integrity of LLDP frames. The second condition is the same as the second condition mentioned to address the first attack. As for the third attack, because a compromised host could interfere with the transmission path of LLDP frames, this problem was solved by using information entropy to calculate the distribution of IP addresses within LLDP frames. If the entropy value falls below a certain entropy threshold, this indicates a hijacking attack. Simulation results demonstrated the effectiveness of

the proposed solutions against mainstream topology attacks.

The researcher in [17] designed a probabilistic graphing model called a dynamic Bayesian network (DBN). In the model, the channel states are modelled by the network users as random variables. The structure of the DBN model is represented by a direct circular vector, which symbolises the legitimate dependence between any pair of variables as a direct vector. The beginning of the vector is the parent variable, and the end of the vector is the child variable. In this model, the conditional probability of each representative random variable and its parents is used, i.e., the conditional probability between the signal received by Alice and the signal received by Bob. This model helps infer leaked information about a key using conditional entropy on the presence of eavesdroppers.

The researcher in [18] explained the difference between a conventional stream cipher and a quantum-noise-randomised stream cipher (such as y00) in terms of conditional probability and entropy. The researchers showed that the ideal Y00 protocol never allows an attacker to extract the keystream as well as the secret key due to overlapping quantum noise caused by the Born rule. They used quantum detection theory to prove that the probability of an attacker successfully obtaining the correct key in the Y00 protocol would never reach 1. They concluded that the probability of shared keys of the Y00 protocol being compromised increases over time, and therefore, a key update procedure by the leftover hash lemma (LHL) should be implemented for the Y00 protocol.

Researchers in [19] have analysed the public opinion on social media. The researchers relied on information theory to derive a general stress index to analyse public opinion. Maximum entropy theory was used to derive this index. To determine the mathematical accuracy of the proposed index, a formula was proposed that results from dividing the expected value by the maximum deviation, and the data were found to be accurate.

The researcher in [20] presented a method for analysing the single-event effects (SEE) and estimating the security of FPGAs based on complex networks. They modelled FPGAs at the register transfer level (RTL) level using module structure network (MSN) and single flow network (SFN). The researchers used five indicators (Degree Centrality, strength centrality, degree centrality, betweenness centrality, clustering coefficient, comprehensive factor) and suggested an evaluation method, is entropy weight method (EWM), to evaluate the impact of the failure of each module in FPGAs. EWM begin by normalising the four indicators, then calculating the entropy value for each indicator. After determining the weight of each factor, a comprehensive factor that evaluates the importance of each module is calculated. To determine the reliability of the FPGA design, the network efficiency was analysed using two modules. Results showed that the proposed model can identify the important module of FPGA circuits and thus countermeasures can be taken as quickly as possible.

Researchers in [21] have proposed an entropy model to evaluate the effectiveness of a video surveillance system for security purposes, such as security control and case investigation. The proposed model calculates the risk entropy of a risk node and takes into account the weighted sum of the membership scores of all factors influencing the surveillance system. Researchers have used entropy from information theory to describe the effectiveness or uncertainty of a surveillance system, meaning that higher uncertainty means lower security effectiveness. The proposed entropy model for risk measurement takes into consideration quantitative and qualitative dimensions of police requirements. Results showed high potential for evaluating computer vision algorithms.

Researchers in [22] have proposed a method for encrypting small weight images and making them secure for transmission in the Internet of Things in wireless networks. This method relies on quantum walking to ensure it is resistant to quantum attacks. The method has been tested using several analyses, including correlation, NIST and Global entropy. The entropy values are equal to 8 in the colour images. The entropy was calculated, and its value was equal to 8. This indicates that the distribution of pixel values in the image is the same before and after encryption, which is an indicator of the effectiveness of the proposed method.

Researchers in [23] have proposed a colour image encryption algorithm which passes in two

stages. The first stage is the permutation process. The second stage is the diffusion process. The researchers evaluated the encryption algorithm based on encryption and decryption speed, key space analysis, and statistical analysis, including entropy. Results showed that the proposed algorithm has high security. Information theory was used once to generate an encryption key and again to evaluate the algorithm's results.

Information Theory

Information theory is a theory based on probability theory. It was founded by the American mathematician Claude Shannon in 1948. Any event in the universe can occur in different ways and is represented by a random variable with its probabilities. Information theory includes a fundamental metric called entropy, which is a measure of the amount of information contained in a random variable. Other metrics in information theory include shared entropy, conditional entropy, mutual information, unit distance, and redundancy.

Uses of Information Theory in Various Fields

1) Cryptography.

Researchers in [24] proposed a new model for evaluating the security of encryption systems in wireless communication networks. This model relied on information theory criteria to assess the security of each encryption system, followed by a game theory model to evaluate the wireless network's security from two perspectives: time and the number of nodes in the network. In [25], researchers proposed a new model for evaluating the security of encryption systems based on a combination of information theory criteria (H(X), H(Y), H(K), H(X|Y)) and a game theory model. The aforementioned criteria were calculated for each encryption system, and then a game theory model was applied to these criteria to calculate the security of each system compared to other comparable systems. In [26], researchers presented a new method, based on information theory criteria and two game theory models, to propose the best strategy for using encryption systems.

2) Networks.

Networks represent the fertile ground in which information theory has grown and flourished. In this section, generalised network classification is explained, and security vulnerabilities are discussed. Information theory has been used to overcome some of their security weaknesses.

1. Cyber-physical networks

They are an extension of embedded networks, consisting of a microcontroller, sensors and actuators. Cyber-physical networks are an integration of computational systems, networks, and physical processes, often operating in real time. Their architecture consists primarily of three layers: physical, network and application [27].

2. Adaptive wireless networks

Wireless ad-hoc networks: a network consisting of a group of nodes (communication devices), which may be mobile. This network lacks a fixed infrastructure and doesn't prioritise the available links between nodes. In this network, direct communication between nodes is not possible, and data is transmitted via individual nodes that transmit packets on behalf of other nodes [28].

MANET: is a group of mobile nodes connected by wireless connections. This network has a dynamic structure made up of self-organising nodes. Each node in the network acts as a router, so data must pass through a group of mobile nodes before reaching its destination [29].

IOV is an extension of the Internet of Things. The network consists of connected vehicles, roadside infrastructure, wireless networks, and central servers for data transmission and content sharing. The IOV collects real-time vehicle information to improve the rate of sending and receiving messages, thereby enhancing operational performance and reducing labour and fuel costs [30].

3. Hybrid and integrated networks

ISTN is a network that combines the advantages of satellite and terrestrial networks. Satellite networks are characterised by their strong disaster tolerance and wider coverage, but network performance is affected by environmental conditions and buildings. While terrestrial networks are characterised by high performance, large capacities, and higher quality of service, they are not applicable in remote areas such as mountains, oceans and other areas.

An ISTN provides an effective solution for continuous connectivity, even in remote areas [31].

SDN-based IIOT is a network that combines the features of the industrial Internet of Things and the architecture of SDN. The IIOT is an extension of the IOT into industrial and commercial domains. Since traditional network architectures do not meet the flexible and variable data processing requirements of the IIOT and the modernisation and expansion of industrial equipment, software-defined networks (SDNs) have been applied to the IIOT environment. SDN architectures offer numerous advantages, including traffic routing adjustment, complex network protocol implementation, ease of operation and maintenance, and scalability to accommodate updated network services [32].

4. Intermittently connected/ offline networks

Offline IOT networks: are closed networks of smart devices that use sensors to collect data from the environment and communicate with each other via local protocols such as Bluetooth, Wi-Fi Direct, and others. The data is received and analysed in a local processing unit, such as a Gateway or edge Node, to make real-time decisions. This data is temporarily stored in a small database and later uploaded to the cloud, if internet access is available, for further analysis and archiving. Its advantages increase data privacy and security, reduce dependency on the internet, lower costsand faster response times-lack of cloud-based analytics, limited remote access. Its disadvantage is integration with other systems, no software or firmware updates and challenges with scaling [33].

Simulation network databases: These are databases used within network simulation systems. These databases include topology models, network traffic datasets, network logs, attack datasets, router/ switch configurations, and datasets for analysing network protocols. These databases are used in many fields, including: enhancing cybersecurity by simulating attacks and testing defenses, training network traffic analysis models based on artificial intelligence and neural networks, developing network systems by testing them and simulating network protocols before implementation on the internet; and education and training, where they are used in university laboratories or training platforms to learn network design and operation without real equipment, simulate industrial systems, and test network-based software [34] .

5. Social and semantic networks

Social networks are a collection of nodes that may have connections with each other. Each node may represent a friend, a customer, or an organisation. Connections between nodes may involve friendship, business relationships, information exchange, or influence. An example might be a network of students in a class who are friends, a group of workers at a company, or a group of fans around an influencer in a particular field [35].

Semantic networks: This type of network is used to represent any type of knowledge that can be expressed in natural language. Knowledge may be an event, an idea, or a situation that has a complex structure. This structure is represented by a network of nodes connected by direct links that represent relationships.

6. Simulation and modelling environments

These are not actual networks. They are achieved through two stages: network modelling and network simulation. Network modelling is a theoretical representation of network behaviour, called a model, and is used to gain a theoretical understanding of the operation of the network or one of its components. Network simulation is the actual implementation of the model using a simulation program such as NS3, Packet Tracer, GNS3, Cisco or Omnet++ to examine the behaviour of the network under various scenarios. Modelling and simulation are used to evaluate the impact of various network traffic models on control performance, on allocation of network resources and on network performance predictability [34].

3) Analysing systems.

Many systems have a significant impact on cybersecurity, including public opinion analysis in multimedia [19], analysing SEE

in Complex Network [20], and evaluating the performance of surveillance camera systems. Such systems require analysis in which information theory criteria play a major role [21].

Forms of Using Information Theory

1- Detecting of (DOS, DDOS, Sybil DDos) attacks: (entropy and joint entropy) of packets are effective detection criteria for different types of Dos attacks because it shows a sharp entropy contrast in comparison with no attack state. The value of entropy is interpreted depending on the type of attack. For example, in a simple DoS attack there is one IP source and therefore the value of entropy is low, while in the case of a DDoS attack the IP addresses are different and therefore the value of entropy is high [1][6]. In DEMI application to detect and mitigate DOS attacks on SDN. a certain number of invalid requests are collected within specific window time and features are extracted. The entropy value is calculated for the extracted destination IP address within time window. If the value is low, it indicates that the packets is centered around a specific IP destination address and it is an indicator for attack. If the value is high, it indicates that the packets is distributed around random specific IP destination addresses. Entropy value is compared with an adaptive threshold mechanism based on (EWMA) [11]. Detecting (DOS) attacks in (ISDN), this work focuses on the confidence level of the node in the routing paths. The trusted model of a single routing node is built based on the comprehensive entropy estimation of all selected characteristics. Detecting (DOS) attacks in (IIOT) based on (SDN). This framework is based on information theory and blockchain. Eight features are selected and are arranged in pairs for each packet, and the mutual information for each pair is calculated. These values are accumulated and stored in a set, sorted from high to low. The first four values are stored in a new matrix, and the second four values are stored in another matrix. The joint entropy of the values in the first matrix is calculated, and the conditional entropy of the values in the second matrix is calculated. The accumulated values for each array are calculated and compared by the controller to check for an attack. (shortly: detected attacks in the intra-domain scheme are uploaded to a smart contract on the blockchain to block these attacks) [10]. Detecting hijacking attacks targeting the SDN topology: a compromised host could interfere with the transmission path of LLDP frames. This problem was solved by using information entropy to calculate the distribution of IP addresses within LLDP frames. If the entropy value falls below a certain entropy threshold, this indicates a hijacking attack [16].

2- Defence scheme against spoofing attacks: A spoofing attack is performed by selecting a target location for spoofing, collecting a list of base stations at the target location, then weakening the signal of the local base stations, and finally spoofing the target's location. The defence scheme relies on generating BS tags for the neighbouring base stations. Entropy is used to generate BS tags with unpredictable frame (high entropy), which has strong resistance to location spoofing attacks [2].

3- Traffic anomaly detection in network: proposed algorithm based on intuitionistic fuzzy time series (IFTS) graph mining. The entropy of capturing packet attributes, which represent random events, is calculated and represents the vertices of the graph; the edge weights of the graph reflect the similarity of the changes in entropy of two vertices connected by an edge. The larger the weight, the more similar the changes. It should be noted that when an anomaly occurs, entropy at both edges or one of them may increase or decrease at the same time [3]. Another method (ED-DBGHSOM) for detecting anomaly network using entropy instead of cumulative error to determine whether a network is growing. Entropy is used to represent the purity of a dataset. Datasets of the same type are transferred to the same neuron, and the entropy value is zero or close to zero. A new concept of entropy, resembling entropy element (REP), is also proposed to calculate the probability of an element occurring within a data vector [7].

4- Malware detection and classification : (MESRF) method based on entropy and wavelet

decomposition. Entropy properties play a significant role in malware detection by the extraction of global and local features of the training data [5]. Detecting malware is an effective first step before applying machine learning algorithms. Two methods based on entropy: 2D-histogram entropy map, converting the input sequence of executable malware into a 2D-image. Applying a sliding window on a 2D-image to compute histogram frequency and then compute histogram entropy. Then construct a fixed 2D entropy feature. The Output of this method can be used by various machine learning. The second method, histogram entropy visualisation, identifies key patterns of malware. It uses the output of the first method (fixed 2D entropy feature), analyses it, and visually reconstructs it [9].

5- Security evaluation: entropy has been used to measure the degree of randomness of the encoding multiple images method. In a normal image, randomness is 8, but after encoding, it was close to 8, which indicates the strength of the encryption method [8]. Entropy is used as an evaluator for the security of noise in accelerometer data. The issue of secure pairing of mobile devices in multimodal transportation (train, car, tram) using accelerometer data. (EKE-DH) protocol ensures secure communication between mobile devices using accelerometer data. Before using accelerometer data in the proposed protocol, the security of the data is analysed using the Hamming distance and entropy. When the entropy value of the accelerometer data is low, this data is easy to predict and is not suitable as a secret key for the protocol, and vice versa [14]. A probabilistic graphing model called a dynamic Bayesian network (DBN) is proposed. In the model, the channel states are modelled by the network users as random variables. In this model, the conditional probability of each representative random variable and its parents is used, i.e., the conditional probability between the signal received by Alice and the signal received by Bob. This model helps infer leaked information about a key using conditional entropy on the presence of eavesdroppers [17]. In terms of conditional probability and entropy, the difference between a conventional stream cipher and a quantum-noise-randomised stream cipher (such as y00) is explained [18]. A new model for evaluating the security of encryption systems in wireless communication networks [24]. A new model for evaluating the security of encryption systems based on a combination of information theory criteria (H(X), H(Y), H(K), H(X|Y)) and a game theory model [25]. a new method, based on information theory criteria and two game theory models, to propose the best strategy for using encryption systems [26].

6- Malicious node detection in ad hoc networks: This approach relies on a combination of cluster-based entropy and machine learning. The LEACH protocol divides the network into clusters. The trust value is calculated for each node based on its behaviour in passing the packets. This trust value is used to calculate the trust entropy to measure the change in trust value over time. The calculated entropy value is compared to a threshold. If the entropy value is greater than the threshold, the node is then considered trusted; otherwise, it is malicious and is detected and blocked [12].

7- Routing protocols: entropy is used to evaluate the trust value of nodes in a specific route. Traditional routing algorithms in MANET select a path based on the fewest hops or the shortest path. A trust entropy routing algorithm was proposed to compute the entropy of a path. The path with the smallest entropy was the highest trust value and will be added to the routing table [13].

8- Security enhancement against data tampering attack: an awareness model is proposed to enhance the operation of communication-based train control (CBTC) systems. If this system is subjected to a data tampering attack, the control commands at the application layer will be overtaken, and the values of movement will be changed, leading to accidents and train collisions. The proposed model used the entropy from information theory in the SVD algorithm to select the dimensions that retain the most information and exclude other less important dimensions in physical and network layers [15].

9- Image encryption: a method for encrypting small-weight images is proposed and making them secure for transmission in IOT. The method has been tested using several analyses, including correlation, NIST and Global entropy. The entropy values are equal to 8 in the colour images. When the encryption process was performed using the proposed method, the entropy was calculated, and its value was equal to 8. This indicates that the distribution of pixel values in the image is the same before and after encryption, which is an indicator of the effectiveness of the proposed method [22]. A colour image encryption algorithm is proposed. Information theory was used once to generate an encryption key and again to evaluate the algorithm's results [23].

10- Analysing systems: The researchers relied on information theory to derive a general stress index to analyse public opinion on social media. Maximum entropy theory was used to derive this index [19]. A method for analysing the single-event effects (SEE) and estimating the security of FPGAs based on complex networks. The researchers used five indicators and suggested an evaluation method, is entropy weight method (EWM), to evaluate the impact of the failure of each module in FPGAs. [20]. An entropy model to evaluate the effectiveness of a video surveillance system for security purposes is proposed. Researchers have used entropy from information theory to describe the effectiveness or uncertainty of a surveillance system, meaning that higher uncertainty means lower security effectiveness. [21].

RESULTS

A review of previous literature concerning the role of information theory parameters in enhancing cybersecurity revealed the following: Information theory plays a significant and effective role in multiple areas of cybersecurity, such as detecting attacks targeting various types of networks; its role in defense schemes designed against network attacks; its role in routing protocols used in networks; its role in security assessment at various levels, including networks, protocols, and encryption systems; its role in image encryption and security assessment; its role in system analysis, such as camera monitoring systems; and its role in detecting flaws in complex networks, such as those used in satellite communications. It was observed that the purpose of using information theory parameters differs in each area. Furthermore, variations in parameter values, whether high or low, have different interpretations depending on the application. For example, in the field of network attacks, a high entropy value indicates a DDoS attack, while a low entropy value indicates a DDoS attack. In defence mechanisms against spoofing attacks, there is a need for unpredictable, random values, hence the high entropy value. In graph mining-based traffic anomaly detection algorithms, changes in entropy values at one end of a graph edge, whether an increase or a decrease, indicate an anomaly in the network. In cluster-based traffic anomaly detection algorithms, entropy indicates the purity of the dataset, which reflects network growth. In image encryption security assessments, an entropy value close to 8 indicates the strength of the encryption method. For evaluating the security of communication protocols in multimodal transportation, entropy is used to assess the accelerometer data; higher randomness indicates more unpredictable data, which can be used for communication encryption. Entropy is used to evaluate the security of encryption systems, with high entropy being preferred, and conditional entropy, which is preferred, is also preferred. In analysing various systems, such as camera monitoring systems, entropy is used to evaluate system efficiency. In complex networks, entropy plays a crucial role in identifying faulty circuits before the problem worsens.

CONCLUSION

It has been observed that information theory plays a significant role in enhancing cybersecurity. Information theory criteria have been applied in various ways, depending on the systems in which they are used, to strengthen cybersecurity. Entropy was used in detecting network attacks. Its role was not as a characteristic of the attack itself, but rather as an indicator of a change in the network's state from attack-free to attack-prone.

Entropy is a measure of randomness and has been used effectively in network defensive schemes against spoofing attacks. Its role focuses on creating

tags for base stations that are difficult for the attacker to predict, and this is the core function of entropy. Entropy is also an effective indicator of similarity that has been used in algorithms for anomaly detection in networks. Entropy is used to represent the purity of a dataset. Conditional entropy is also very important for determining the information stolen from the transmitted ciphertext; the less information there is, the stronger the encryption algorithm. The concept of randomness is crucial in evaluating image encryption methods. Each image has a specific entropy value depending on the colours it contains. If the entropy value of the image after encryption is equal to its value before encryption, this is a strong indicator of the encryption method's effectiveness. It has been observed that several indicators exist for detecting an attack on routing algorithms, such as shorter paths or fewer hops, but recent research focuses on using entropy to examine path reliability. The lower the path's entropy, the more reliable the path is within the network's routing algorithms. Security enhancement against data tampering attacks in CBTC systems, entropy is used in dimension reduction in the physical and network layers. Different entropy measurements, whether small or large, have had a significant impact on improving cybersecurity. This leads us to apply information theory more broadly in all areas of cybersecurity, and indeed in various other areas of life.

REFERENCES

[1] J. Li, M. Liu, Z. Xue, X. Fan and X. He, RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things, IEEE Access, Vol. 8, pp. 36191-36201, Mar. 2020.

[2] A. Ye, Q. Li, Q. Zhang and B. Cheng, Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags, IEEE Access, Vol. 8, pp. 39768-39780, Mar. 2020.

[3] Y. Wang, J. Wang, X. Fan anf Y. Song, Network Traffic Anomaly Detection Algorithm Based on Intuitionistic Fuzzy Time Series Graph Mining, IEEE Access, Vol. 8, pp. 63381-63389, Mar. 2020.

[4] K.Guo, D. Wang, H. Zhi, Y. Lu and Z. Jiao, A Trusted Resource-Based Routing Algorithm With Entropy Estimation in Integrated Space-Terrestrial Network, IEEE Access, Vol. 8, pp. 122456- 122468, Mar. 2020.

[5] H. Guo et al., File Entropy Signal Analysis Combined With Wavelet Decomposition for Malware Classification, IEEE Access, Vol. 8, pp. 158961- 158971, Sep. 2020.

[6] J. Li, Z. Xue, C. Li and M. Liu, RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles, IEEE Access, Vol. 9, pp. 11296- 11305, Sep. 2021.

[7] X. Qu, et al., Entropy-Defined Direct Batch Growing Hierarchical Self-Organizing Mapping for Efficient Network Anomaly Detection, IEEE Access, Vol. 9, pp. 38522-38530, Mar. 2021.

[8] M. Tanveer et al., Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box, IEEE Access, Vol. 9, pp. 73924- 73937, May. 2021.

[9] B. Bake, S. Duh, D. Bake, D. Kim and D. Hwang, Histogram Entropy Representation and Prototype Based Machine Learning Approach for Malware Family Classification, IEEE Access, Vol. 9, pp. 152098- 152114, Nov. 2021.

[10] S. Jian and J. Mengnan, A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT, Chinese Journal of Electronics, Vol. 32, pp. 531- 541, May. 2023.

[11] L. Eliyan and R. Pietro, DeMi: A Solution to Detect and Mitigate DoS Attacks in SDN, IEEE Access, Vol. 11, pp. 82477- 82495, Aug. 2023.

[12] S. Kanthimathi, Exploring Machine Learning Algorithms for Malicious Node Detection Using Cluster-Based Trust Entropy, IEEE Access, Vol. 12, pp. 137913- 137925, Oct. 2024.

[13] X.Wang, P. Zhang, Y. Du and M. Qi, Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network, IEEE Access, Vol. 8, pp. 47676-47693, Mar. 2020.

[14] B. Groza, A. Berdich, C. Jichici and R. Mayrhofer, Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport, IEEE Access, Vol. 8, pp. 9246-9259, Jan. 2020.

[15] Q. Li, B. Bu and J. Zhao, A Novel Hierarchical Situation Awareness Model for CBTC Using SVD Entropy and GRU With PRD Algorithms, IEEE Access, Vol. 9, pp. 132290-132300, Oct. 2021.

[16] Y. Gao and M. Xu, Defense Against Software-Defined Network Topology Poisoning Attacks, TSINGHUA SCIENCE AND TECHNOLOGY, Vol. 28, pp. 39- 46, Feb. 2023.

[17] X. Huang, N. Ansari, S. Huang and W. Li, Dynamic Bayesian Network Based Security Analysis for Physical Layer Key Extraction, IEEE Com Soc, Vol. 3, pp. 379- 390, Feb. 2022.

[18] T. Iwakoshi, Analysis of Y00 Protocol Under Quantum Generalization of a Fast Correlation Attack: Toward Information-Theoretic Security, IEEE Access, Vol. 8, pp. 23417-23426, Feb. 2020.

[19] H. Zhang, R. Jin, Y. Zhang and Z. Tian, A Public Psychological Pressure Index for Social Networks, IEEE Access, Vol. 8, pp. 23457-23469, Feb. 2020.

[20] M. Wang, T. Zhang, J. Wang, S. Zhou and L. Kong, SEE Fault Sensitivity Analysis and Security Reinforcement Design for FPGA Circuits Based on Complex Network, IEEE Access, Vol. 8, pp. 95618- 95628, June 2020.

[21] H. Zhang, P. Li, Z. Du and W. Dou, Risk Entropy Modeling of Surveillance Camera for Public Security Application, IEEE Access, Vol. 8, pp. 45343- 45355, Mar. 2020.

A. El-Latif et. al, Providing End-to-End Security Using Quantum Walks in IoT Networks, IEEE Access, Vol. 8, pp. 92687-92696, May 2020.

[22] J. Wang, J. Li, X. Di, J. Zhou and Z. Man, Image Encryption Algorithm Based on Bit-Level Permutation and Dynamic Overlap Diffusion, IEEE Access, Vol. 8, pp. 160004-160024, Sep. 2020.

[23] S. Sadkhan and D. Reda, Cryptosystem Security Evaluation Based on Diagonal Game and Information Theory, 2018 International Conference on Engineering Technologies and their Applications (ICETA), IEEE, pp. 118-123, Sep. 2018.

[24] S. Sadkhan and D. Reda, A Proposed Security Evaluator for Cryptosystem Based on Information Theory and Triangular Game, IEEE, pp. 306-311, Nov. 2018.

[25] S. Sadkhan and D. Mohammad, Hybrid Strategies for Choosing Suitable Cryptosystem Based on Game and Information Theories, Fifth International Engineering Conference on Developments in Civil & Computer Engineering Applications 2019 - (IEC2019), IEEE, pp. 95-100, 2019.

[26] K. Pan, F. Yang, Z. Feng and Q. Pan, Attack Reconstruction for a Class of Cyber-physical Systems with Altering Load*, 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), pp. 78- 83, August 2021.

[27] R. Ramanathan and J. Redi, A BRIEF OVERVIEW OF AD Hoc NETWORKS: CHALLENGES AND DIRECTION, IEEE Communications Magazine 50th Anniversary Commemorative Issue, pp. 20-22, May 2002.

[28] U. Srilakshmi et al., An Improved Hybrid Secure Multipath Routing Protocol for MANET, IEEE Access, Vol. 9, pp. 163043-163053, Dec. 2021.

[29] T. Li, C. Li, J. Luo and L. Song, Wireless recommendations for internet of vehicles: Recent advances, challenges, and opportunities, Intelligent and Converged Networks, Vol. 1, pp. 1-17, May 2020.

[30] H. Sai et al., Early warning of core network capacity in space-terrestrial integrated networks, Journal of Systems Engineering and Electronics, Vol. 35, pp. 855-864, Aug. 2024.

[31] S. Jian and J. Mengnan, A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT, Chinese Journal of Electronics, Vol. 32, pp. 531-541, May 2023.

[32] O. Diallo, J. Rodrigues, M. Sene and J. Lioret, Simulation framework for real-time database on WSNs, Journal of Network and Computer Applications, Vol. , pp. 1-11, July 2013.

[33] J. Baras, MODELING AND SIMULATION OF TELECOMMUNICATION NETWORKS FOR CONTROL AND MANAGEMENT, Proceedings of the 2003 Winter Simulation Conference, pp. 431-440, 2003.

[34] K. Musial and P. Kazienko, Social networks on the Internet, https://link.springer.com/, Vol. 16, pp. 31-72, 2013.

[35] F. Lehmann, SEMANTIC NETWORKS, ComputerJ Math. Applic., Vol. 23, pp. 1-50, 1992.