MSDAR: Multi-Stage Dynamic Architecture Intrusion Detection System

Ahmed M. ElShafee[1]
Ahram Canadian University
Cairo, Egypt

Marianne A. Azer[2]
National Telecommunication Institute
Nile University, Cairo, Egypt

***Abstract*—Ad hoc networks have been through extensive research in the last decade. Even with their desirable characteristics, major issues related to their security need to be considered. Various security solutions have been proposed to reduce the risks of malicious actions. They mainly focus on key management, authentication, secure localization, and aggregation techniques. These techniques have been proposed to secure wireless communications but they can only deal with external threats. Therefore, they are considered the first line of defense. Intrusion detection systems are always required to safeguard ad hoc networks as such threats cannot be completely avoided. In this paper, we present a comprehensive survey on intrusion detection systems in ad hoc networks. The intrusion detection systems and components and taxonomy as well as different implementations and types of IDSs are studied and categorized. In addition, we provide a comparison between different Intrusion Detection Systems' architectures. We also propose a Multi Stage Dynamic Architecture intrusion detection system (MSDAR), designed with a multi-stage detection approach making use of both signature-based and anomaly detection benefits. Our proposed intrusion detection system MSDAR is featured by its dynamic architecture as it can be deployed in the network using the Distributed Hierarchical Architecture. The viability and performance of the proposed system MSDAR are tested against the Distributed Denial of Service Attacks through simulations. Advanced performance parameters were used to evaluate the proposed scheme MSDAR. Experimental results have shown that the performance of MSDAR improves by using multiple stages of different detection mechanisms. In addition, based on simulations, the Detection Rate increases when the sensitivity level increases.**

***Keywords*—Ad hoc networks; attacks; DDoS; intrusion detection; security**

I. INTRODUCTION

Emerging technologies have contributed in revolutionizing our daily life. To mention a few, Artificial Intelligence (AI) [1], Blockchain, cryptocurrencies [2], Internet of Things (IoT) [3], cloud computing, and wireless technology. Wireless technology is critical to today's communications [4], and essential to developing technologies within the next years. Wireless communications are almost based on ad hoc or special purpose connections. Mobile Ad hoc Networks (MANETs) are key players in the future of wireless communication [5]. They consist of distributed nodes without any predetermined infrastructure [6]. The lightweight mobile devices have the capabilities of sensing and processing received information [7]. The devices have a limited transmission range that needs intermediate nodes to reach other far nodes. Due to their special features, ad hoc networks are susceptible to a wide range of attacks [8], exterior and interior threats and misbehaving modes [9]. Some of these attacks are initiated to deprive legitimate users of network services. Other attacks have the objective of gaining unauthorized access to network resources [10].

MANETs have many different challenges regarding designing security solutions due to their vulnerability to eavesdropping, lack of trusted management, limited computation capabilities, and power sources which increase their vulnerability to Denial of Service (DoS) attacks and also can become incapable of running heavy security algorithms. Due to the open, self-organized, infrastructure-less environment of MANETs, there is a chance that trusted nodes to be hijacked. Therefore, any security solution should be designed to defend the network against both insider and outsider attacks. In MANETs, insider attacks are more problematic and difficult to overcome. Security solutions for ad hoc networks are considered to be one of the most active and attractive research areas. Researchers mainly focus on key management [11], authentication, secure localization, and aggregation techniques to secure wireless communications [12]. The current security solutions can only deal with external threats, and therefore they can be considered the first line of defense. However, insider attackers that already exist within the first perimeter of defense can penetrate the whole network and cause severe damage. Therefore, Intrusion Detection Systems are considered the second line of defense as they come into action after the intrusion has already occurred [13]. There are two types of Intrusion Detection Systems (IDSs), signature based detection IDS, and anomaly-based detection IDS [14]. Signature-based IDSs (misuse detection) require a knowledge base containing the behavioral patterns of different attacks. When the IDS detects a certain pattern that refers to an attack, it alerts the network's users against this specific attack. The main disadvantage in such implementation is that only known attacks are caught and reported. This may surge the percentage of false negatives. On the other hand, anomaly detection, IDSs (behavior-based detection) are not designed to catch threats using their signature or pattern. They are developed to learn the normal behavior patterns of both users and network applications to discover and report any altered patterns. In anomaly-based IDSs, new and unknown attacks can be detected and reported whenever they occur. However, any abnormal benign behaviors will be caught and reported as

new threats. This may increase the percentage of false positives.

This research introduces a newly developed trust-based IDS for wireless ad hoc networks. The proposed Multi Stage Dynamic Architecture Intrusion Detection System (MSDAR) takes into consideration multistage detection mechanisms to increase its capability to detect different types of intrusions. The first and third stages are based on anomaly detection, while the second is signature-based detection. In the third stage, an additional parameter is used, it is called the sensitivity level.

The contributions of this paper are as follows.

1) The Intrusion Detection Systems components and taxonomy as well as different implementations and types of IDSs are studied and categorized. The study's objective is to understand the algorithms and design parameters and their impact on performance and functionality.

2) A comparison between different Intrusion Detection Systems' architectures from the points of view of complication, precision, scalability, and possibility of failure is provided.

3) The taxonomy of IDSs' architectures, detection algorithm, and additional design parameters is presented.

4) Our proposed intrusion detection system architecture and the operational algorithm are explained in detail. The proposed MSDAR is designed with a multi-stage detection approach making use of both signature-based and anomaly detection benefits. Simulation analysis methodology, simulation parameters, simulation metrics used for performance evaluation, and simulation results are also presented and discussed in detail.

The remainder of this paper is organized as follows: In Section II, we give an overview of the related work done for securing ad hoc networks using Intrusion Detection Systems. Section III gives an insight into our implementation. Section IV presents the simulation results and evaluation of our proposed scheme MSDAR. Section V is focused on discussing the results and mentioning the limitations Of MSDAR. Finally, Section VI concludes the paper and presents future directions are presented.

II. Related Work

Intrusions are any kind of unauthorized or unapproved activities within the network. Intrusion Detection Systems are schemes and tools, used to discover, assess and report intrusions that may compromise the network. IDSs should continuously adapt and improve, to be able to discover new attacks and attack strategies. Many factors have motivated the development of IDSs. First, the presence of security flaws and vulnerabilities in a complex system makes it susceptible to malicious intrusions. Second, is the inefficiency of most of the prevention techniques that were designed and implemented to prevent possible attacks. Third, the exposure to insider attacks is expressed to be much more harmful than outsider attacks, even in most secure systems. Finally, newly emerged attacks need considerably advanced security solutions. This makes IDSs an attractive and important research area. For this research, different implementations and types of IDSs are studied and categorized in this section. The study's objective is to understand the algorithms and design parameters and their impact on performance and functionality, to overcome any unexpected flaws in our new proposed technique MSDAR. This section is organized as follows. Structural components and building blocks are introduced in Section A. Section B gives an insight into IDSs' architecture taxonomy. Supplementary design parameters and their taxonomy are introduced in section C.

A. Intrusion Detection Systems' Components

Because of their common goals, most of IDSs share the same structural patterns [15]. Data collecting and formatting, analysis and detection, and reaction mechanism units are the three primary parts of any IDS. The main components of the intrusion detection systems are depicted in Fig. 1. Various data types from different sources are collected, formatted and sorted at the data collection and formatting unit and then delivered to the analysis and detection unit. Collected data is analyzed and processed and then compared to the normal system behavior in anomaly-based IDS, or the signature of known attacks in signature-based IDS, or finally the well-defined specifications of a program or protocol in specification-based IDS [16]. After an action is detected as malicious, it is reported to the response mechanism. The response mechanism is defined according to the designed response policy. Different responses can only be categorized into two groups; passive responses and active responses. The passive response is done by simply notifying the authorized entity of the identified malicious action or intrusions detected. On the other hand, an active response is any form of action aiming to mitigate the threat or expected damage resulting from an intrusion or attack. This can be done by terminating network connections for certain periods or blocking IP addresses/Physical addresses linked to the attack. The response policy should also illustrate the response period as it can be either permanent or temporary. IDSs with active response mechanisms can also be aliased as Intrusion Prevention Systems (IPSs).

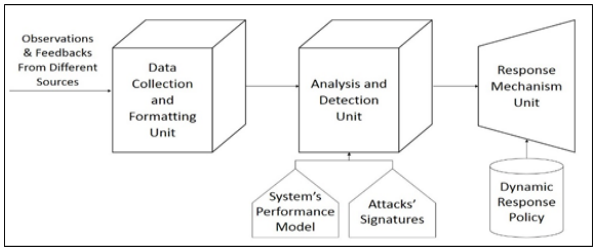


Fig. 1. The Intrusion Detection System's Building Blocks.

B. Intrusion Detection Systems Architectures Taxonomy

Intrusion detection systems can be deployed in the network using different architectures [17]. These architectures can be classified into two broad categories; Standalone, and collaborative, as shown in Fig. 2. Early IDSs were implemented as stand-alone systems having only local monitors and analysis units at each node. Local monitors and analysis units serve only their host nodes by detecting abnormal events according to the predefined detection policy. The response against any action is addressed and limited to the

node's level with no extra extension. Stand-alone IDSs are not immune against distributed attacks and they can't be reliable for detecting malicious events occurring simultaneously at different locations inside the network. Therefore, there is a need for Collaborative IDSs. In collaborative architectures, an IDS enforces cooperation between monitors to provide a considerably more scalable and accurate model than stand-alone IDS. Collaborative IDS are also classified according to the communication model between both monitor units and analysis units as depicted in Fig. 2. Collaborative IDSs classification includes four subcategories, centralized, decentralized, distributed, and finally, our newly proposed architecture that is illustrated in this paper; hierarchically-distributed. Centralized IDSs, depend on one single centralized analysis unit in addition to several distributed monitoring units at each node or entity in the network. Two main disadvantages of such IDSs are the scalability limitations and the Single Point of Failure (SPoF). This is because the single analysis unit can handle only a limited number of monitoring units and it can be an easy target for direct attacks to disable the entire functionality of the intrusion detection system. Decentralized IDSs make use of multiple analysis units distributed in different locations within the network. Each analysis unit is responsible for accumulating, aggregating, and analyzing data from different monitoring units. Finally, a head analysis unit on top of all other analysis units receives this information, to make nondiscriminatory decisions regarding network entities and events. Such architecture supports scalability and overcomes the bottleneck congestion presented in centralized IDSs. In Distributed IDSs, each entity in the network is equipped with a monitor unit and an analysis unit. Each node shares its information with its peers in a completely distributed model. Collected data are organized and analyzed among all nodes. In Distributed IDS architecture, both congestion and SPoF disadvantages are avoided. However, an extra processing requirement is added to each node within the network. This additional requirement may consume extra processing and power capabilities during intrusion detection activities which in turn minimize the nodes' capabilities required to process normal flow. Therefore, a new architecture is proposed to overcome the disadvantages mentioned above. It is based on both Distributed and Hierarchical Architecture (DHA-IDS) as shown in Fig. 3.

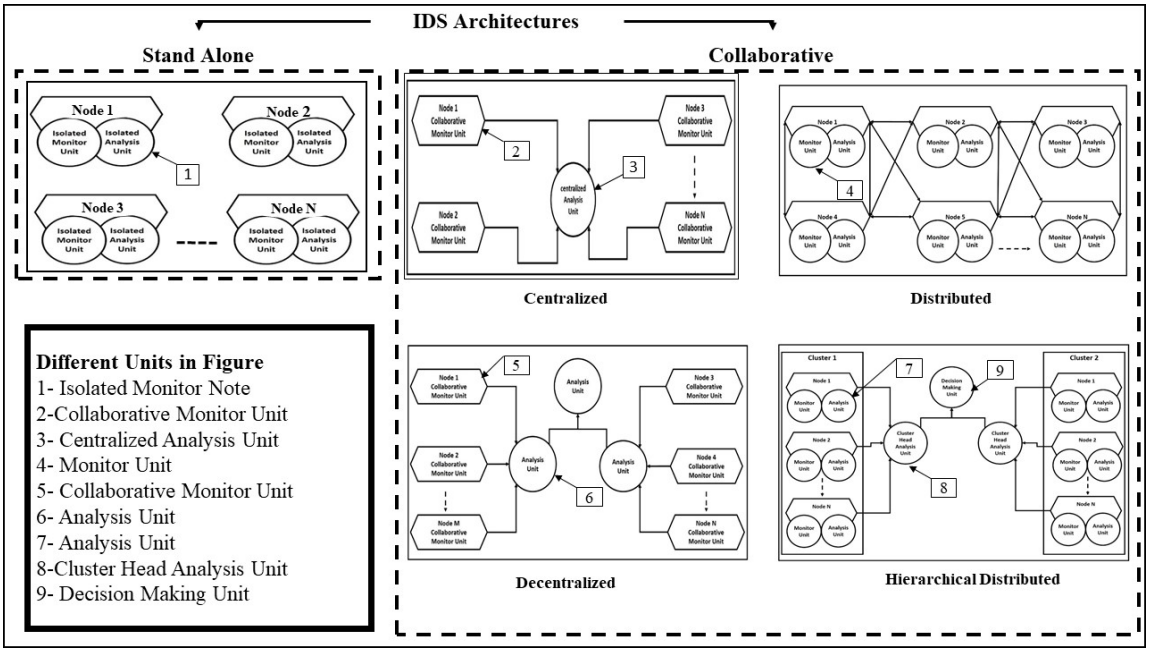


Fig. 2. Extended Intrusion Detection Systems Architectures Taxonomy.

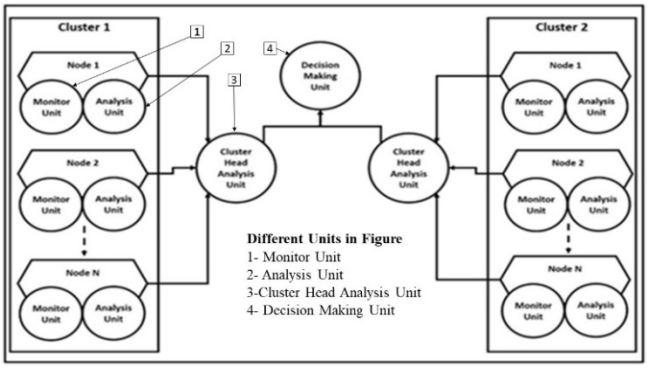


Fig. 3. Proposed Distributed Hierarchical Intrusion Detection System (DHA-IDS) Model.

In DHA-IDS, each node has its own monitor and analysis units. Each node is responsible for monitoring and analyzing only data collected by itself, then it forwards the analyzed data about different network activities to the cluster head analysis unit directly above it. Each cluster head analysis unit is responsible for collecting data from the nodes within its cluster. It then runs the second phase of processing and analyzing to correlate all collected information. At the end, each cluster head analysis unit forwards the correlated information to the response unit which is responsible of deciding a proper action related to detected intrusions. If an attack is directed to the response mechanism unit, one of the cluster head analysis units will become responsible of replacing the response mechanism unit. Similarly, in case the attack is extended to the cluster heads, each node will depend on its information and make its own decision regarding any suspected action. Therefore, this proposed DHA-IDS can perform in the worst attack conditions and it can degrade its architectural level from Distributed Hierarchical to Standalone, in order to retain the system's self-robustness. Furthermore, the new proposed architecture overcomes many disadvantages of different architectures mentioned above like; bottleneck congestion, SPoF, processing and power overheads. Table I compares between the different architectures presented in this section and the proposed DHA-IDS. They are compared based on complexity, accuracy, scalability, and risk of failure.

TABLE I. COMPARISON BETWEEN DIFFERENT IDSS' ARCHITECTURES USING THE FOLLOWING CRITERIA: COMPLICATION, PRECISION, SCALABILITY, POSSIBILITY OF FAILURE ON THREE LEVELS, LOW (L), MEDIUM (M), HIGH (H)

Architecture	**Complexity**			**Precision**			**Scalability**			**Possibility of Failure**		
Classification	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Stand alone	√			√					√	√		
Centralized	√					√	√					√
Decentralized		√		√					√	√		
Distributed			√		√				√		√	
Distributed-Hierarchical		√				√			√	√		

C. Intrusion Detection Systems Design Parameters Taxonomy

Different parameters are taken into consideration when a new IDS is designed. These parameters influence the IDS performance. Some of these parameters are presented in the following sections.

1) Source of data: According to the source of data, IDSs can be classified as Host-based, Network-based, and Hybrid. In stand-alone architectures, data is collected and analyzed locally from each node independently. Another approach is collaborative security, which is accomplished by multiple correlated sources. Data can be collected either locally and independently, or globally from each node (host-based) in the network then the collected data can be correlated and analyzed in a holistic form [18]. In such IDSs, monitoring units are deployed locally in the host to detect host-targeted attacks. Examples of such attacks are the ones aiming to exhaust the hosts' resources or gain unauthorized access to systems' components and data. Data can also be collected from network traffic (network-based) instead of nodes' local data [19]. Monitoring units are deployed in firewalls, or routers to capture all network packets. This information can help to detect different threats and possible attacks and spot abnormal activities in the network. Finally, some IDSs depend on their design and implementation on both sources of data, host-based, and network-based. This type of IDS is described as (hybrid-sourced). Hybrid-sourced IDSs can detect various types of attacks targeting any of the host or network components.

2) Scheduling of analysis: The intrusion detection process can trail different schedules (real-time, offline). In real-time analysis [20], data is collected, then immediately correlated and analyzed. Instantly, an appropriate decision is taken regarding the detected behavior. On the other hand, offline analysis [21] is performed after all nodes forward their collected data to the analysis unit. While the data is being analyzed, the nodes pursue their normal operation. Whenever they receive a decision concerning the network activities, they act accordingly.

3) Initiation: Nodes in IDSs can voluntarily participate in the intrusion detection process like in proactive systems. Monitoring units collect data that is automatically forwarded to analysis units. On the contrary, in driven systems, nodes wait for a direct request to send their own data regarding any activity in the network. Also, the passive nodes don't request neighboring nodes' data. They only receive data passing by their perimeter passively.

4) Types of shared data: Collaborative IDSs depend on sharing data among the network elements. There are three types of data: Raw, partially processed, and fully processed. Raw data is collected by nodes that are not equipped with any analysis units. Data is then forwarded to other nodes with higher processing capabilities for analysis. Environmental data and behavior logs are examples of raw data. In case of partially processed data, nodes are more powerful, so they can be used to minimize the traffic overhead due to forwarding every single piece of raw data at each node in the network. Also, IDSs make use of partially processed data to minimize the processing capabilities required by each node in the IDS's higher levels. Finally, the existence of malicious or abnormal activity in the network is determined by the fully processed data. Therefore, confirmed intrusions, attacks, decisions, and alerts regarding a node can be considered fully processed data. Fig. 4 depicts the taxonomy of IDSs' Architectures, detection algorithms, and additional design parameters. Table II summarizes the classification and the comparison between some IDSs that have been proposed in the literature with respect to different parameters such as Communication architecture, and detection algorithms. This is in addition to other design parameters such as data source, shared data type, scheduling of analysis, and response mechanism point of view.

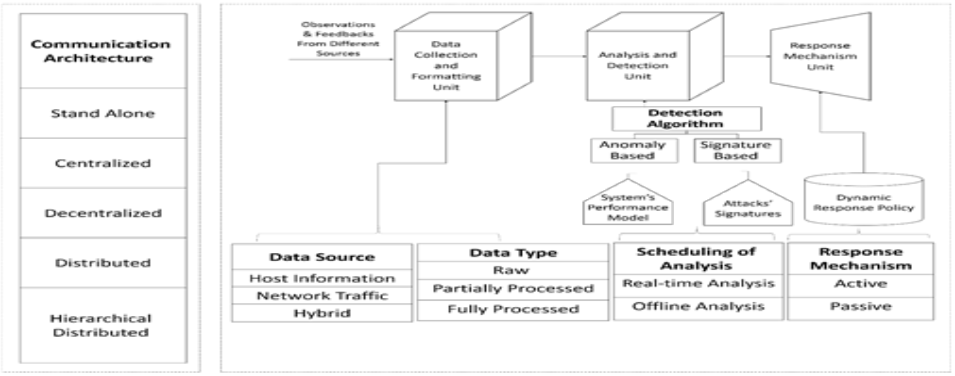


Fig. 4. Taxonomy of IDSs' Architectures, Detection Algorithm and Additional Design Parameters.

TABLE II. COMPARISON BETWEEN INTRUSION DETECTION SYSTEMS BASED ON THEIR DESIGN PARAMETERS

ntrusion Detection System			**DIDS [22]**	**CRIM [23]**	**DIDMA [24]**	**GRIDS [25]**	**HIDE [26]**	**EMERALD [27]**	**INDRA [28]**	**LARSID [29]**	**DOMINO]30]**	**SNORT [31]**	**WORMI -NATOR [32]**	**QUI CK SAND [33]**	**PEREZ [34]**	**LIDS [35]**
Communication Architecture		**Centralized**	√	√	√											
		Decentralized				√	√	√							√	√
		Distributed							√	√	√	√	√	√		
Detection Algorithm		**Signature Based**		√	√	√		√			√	√		√	√	√
		Anomaly Based	√				√	√	√	√			√			
Additional Design Parameters	**Data Source**	**Host Based**		√	√	√		√		√				√		√
		Network Traffic						√				√				
		Hybrid	√				√		√		√		√		√	
	Data Type	**Raw**		√						√						
		Partially Processed	√		√	√					√				√	
		Fully Processed					√	√	√			√	√	√		√
	Analysis Schedule	**Real-time**				√	√		√	√		√				
		Offline	√	√	√			√			√		√	√	√	√
	Response Mechanism	**Active**							√		√	√				
		Passive	√	√	√	√	√	√		√			√	√	√	√

III. PROPOSED SYSTEM ARCHITECTURE

This section presents our proposed system architecture and operational algorithm. The proposed MSDAR is designed with a multi-stage detection approach. The first stage is implemented using anomaly detection with a classifier mechanism. The system in this stage has a statistical prediction of most successive events in the network. The analysis unit compares the current event to the pre-predicted event, if they match; then the system is considered to be operating in its normal state. If the current event doesn't match any of the pre-predicted events, then it will be considered an anomaly. The second stage is implemented using a signature-based detection mechanism. At this phase, the analysis unit compares the current event - detected as an anomaly in the first stage - to the predefined attacks behaviors' and signatures' profiles. Therefore, an anomaly detected in the first stage is considered as the audit data for the second stage. The third stage and the following ones are implemented using anomaly detection with a classifier mechanism that has an additional parameter taken into consideration. This parameter is the Sensitivity level of upcoming comparisons. Sensitivity Level SL is incremented each time the system needs to make further investigations regarding the group of events suspected to be an intrusion and correspondingly to minimize the false positive intrusion percentage. The state diagram of the proposed system MSDAR is depicted in Fig. 5. MSDAR follows the standardized structure of known collaborative IDSs. Data collection and formatting units are the first components of its structure. It is designed to have various data sources distributed through the

network, and at each host within the network perimeter. Monitor unit and mini-analysis unit are implemented at different data sources. Collected and formatted data are forwarded to the main analysis and detection unit where the analysis processes follow the scheme shown in the flow chart depicted in Fig. 6. Finally, the response unit has the role of propagating a proper response related to any detected intrusion. The response is decided according to the designed response policy. The active response is considered against any intrusive action.

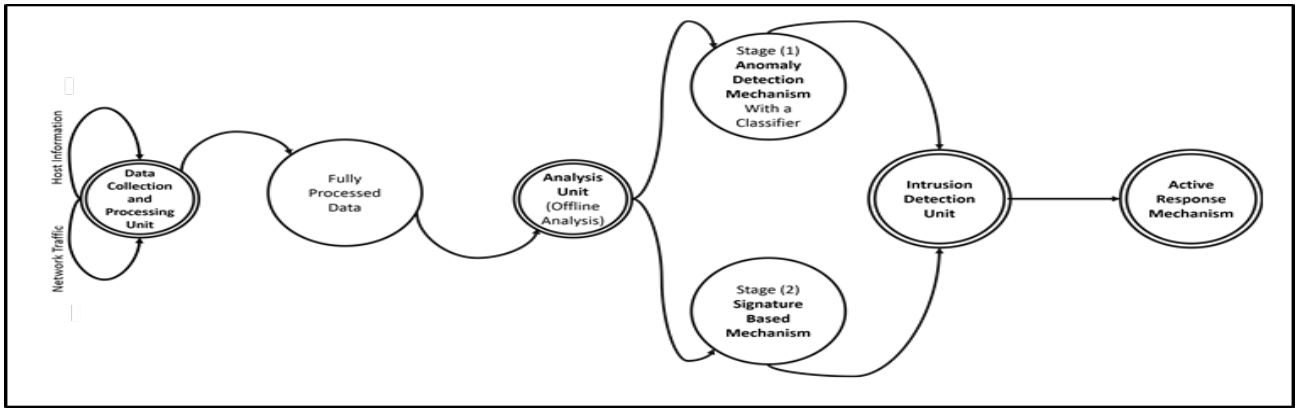


Fig. 5. State Diagram of Multi Stage-Dynamic Architecture-IDS (MSDAR).

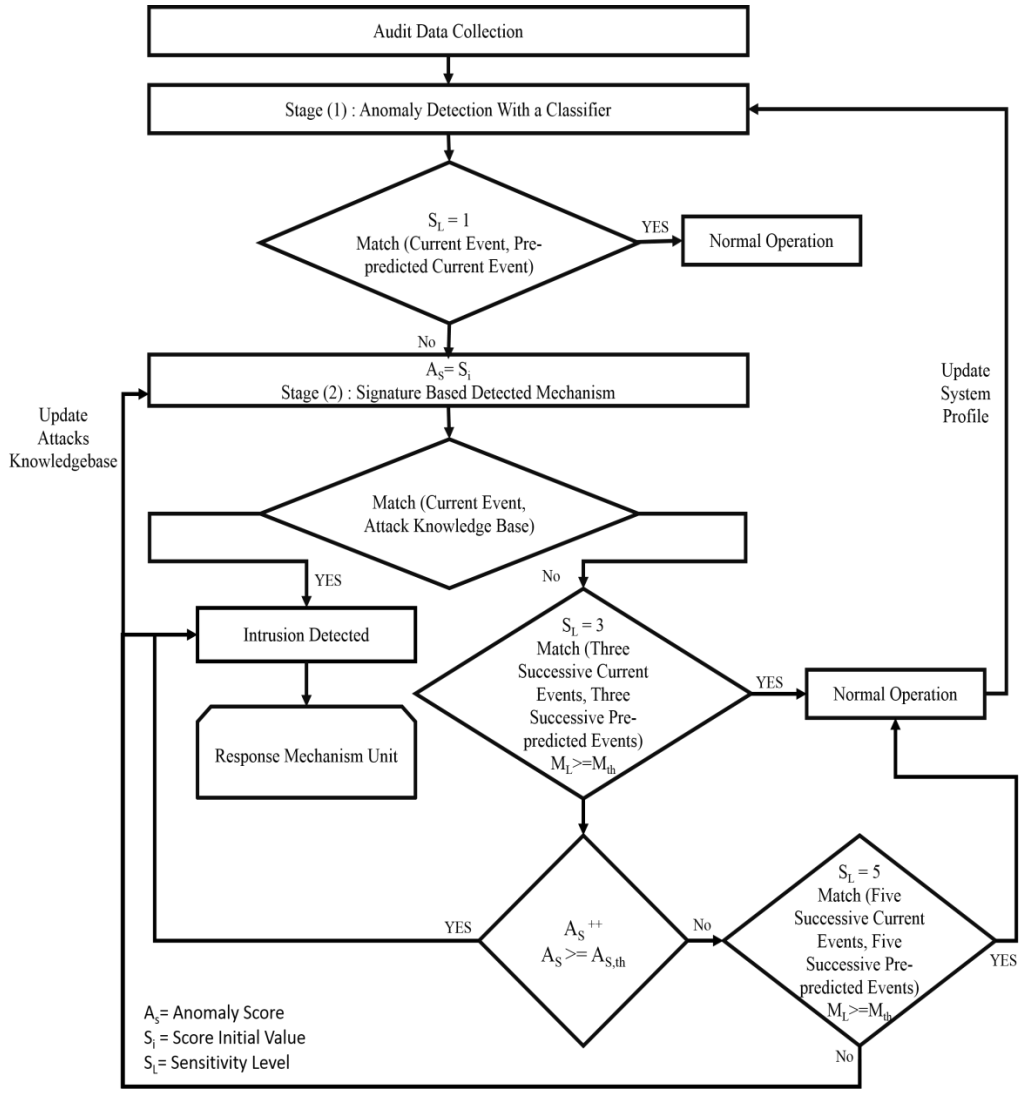


Fig. 6. FULL Operational Flow Chart of Multi Stage-Dynamic Architecture-IDS (MSDAR).

IV. MSDAR Simulation Results

This section describes the technique used to evaluate MSDAR performance, using the OMNET++ Simulator. The simulated network consists of 80 nodes acting as routers, two workstations acting as data sources, and one application server acting as the victim. All nodes are assigned static IP addresses to enable the possibility of tracking routing tables at each node.

For the simulation, AODV is used as the routing protocol. Fig. 7 summarizes the simulation parameters. For the attack scenario, a certain percentage of nodes are manipulated to act as malicious attackers. The monitored systems' behavioral statistics are then gathered. The following statistics are included: total packets transferred, total packets received, total packets deleted, total packets changed, latency, total connections to the victim node, and average throughput… etc).

A. Simulation and Analysis Methodology

Each event that scores greater than the predefined threshold is marked as an intrusion. Subsequently, a proper action using the MSDAR response mechanism is initiated. In the final stage of the simulation process, overall network performance evaluation is presented in graphs to validate MSDAR's ability to detect the existence of intrusive actions. The following tables present the parameters used for the simulation, testing scenario, and collect statistical data respectively. To assess the efficacy of our suggested system, it is important to measure its ability to distinguish between intrusive and non-intrusive activities, with a minimum number of false alarms. In our evaluation, we adopted the approach in [36]. The metrics used are defined in Table III [36]. The previously mentioned singular metrics were used to form new performance measures. These performance measures are introduced in Table IV [37]. Some researchers consider DR and TPR as the same measure: the proportion of intrusive events that were identified as attacks to all other normal events [37].

To have a fair comparison between IDSs performance, the authors in [36] proposed a metric called Capability of Intrusion Detection (CID) based on some of the metrics mentioned in Table IV, according to (1).

$$CID = -B(1-\beta)\log(PPV) - B(\beta)\log(1-NPV) - (1-B)(1-\alpha)\log(NPV) - (1-B)(\alpha)\log(1-PPV) \quad (1)$$

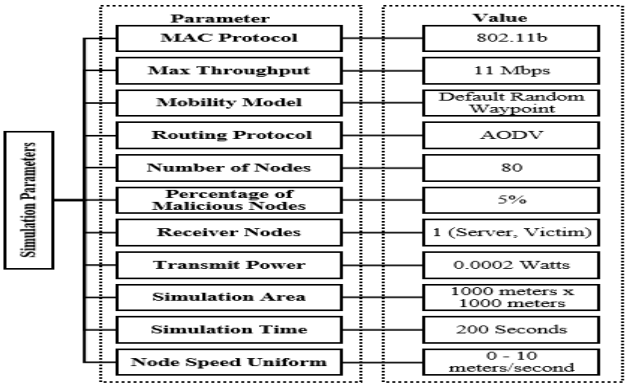


Fig. 7. Simulation Parameters.

TABLE III. Metrics Defined for IDS's Performance Evaluation [36]

Metric	Meaning	Explanation
FP	False Positive.	The probability of having an alert while no intrusion occurs.
TP	True Positive.	The likelihood of receiving an alarm during an incursion.
FN	False Negative.	The likelihood of not receiving an alarm when an incursion occurs.
TN	True Negative.	The likelihood of not receiving an alert if no incursion happens.
PPV	Positive Predictive value.	The likelihood that an intrusion results in an alert.
NPV	Negative Predictive Value.	The likelihood of no inclusion results in no alert.
B	Base Rate.	The likelihood of an intrusion in the audit data gathered.

TABLE IV. Advanced Performance Measures for IDS's Evaluation [37]

Performance Parameter	Definition	Equation	Value Range
Classification Rate (CR)	The ratio between accurately classified events and the total number of events.	$\frac{TP+TN}{TP+TN+FP+FN}$	CR > 0 CR < 1
Detection Rate (DR)	The proportion of properly identified attacks to the total number of intrusive occurrences.	$\frac{TP}{TP+FN}$	DR > 0 DR < 1
False Positive Rate (FPR) (α)	The proportion of non-intrusive events detected as attacks to the total number of non-intrusive occurrences.	$\frac{FP}{FP+TN}$	FPR > 0 FPR < 1
True Positive Rate (TPR) (1-FNR) (1-β)	The proportion of intrusive events detected as attacks to the total number of regular occurrences.	$\frac{TP}{FP+TN}$	TPR > 0 TPR < 1

B. Simulation Results

One of the most difficult tasks is data gathering [38]. In our simulations, we used the dataset DARPA 2000 Lincoln Laboratory Scenario (LLDDoS) 2.0 which is provided by MIT [39]. It consists of a DDoS attack run by five attackers. A number of simulation sessions are used to carry out this assault scenario. Over time, these sessions were organized into 5 attack stages. MSDAR has been simulated and tested against LLDDOS 2.0.2. The following graphs have been deduced from the simulations. Fig. 8 illustrates the point-to-point throughput during the five time phases of the attack. It shows five peaks at each attack incidence. Fig. 9 illustrates the number of connections directed at the victim node. It can be noticed that the number of connections is exponentially increasing with time. Fig. 10 and Fig. 11 demonstrate the average throughput of the network and received throughput at the victim node respectively. The Receiver Operating Characteristic (ROC)

Curve [40] is the detection rate as a function of the false positive rate and the corresponding calculated CID curve as a function of false positive rate for the different stages (sensitivity levels) of MSDAR respectively. Fig. 12 depicts the ROC of our scheme. From Fig. 12, it can be concluded that the Detection Rate increases when the sensitivity level increases. For αavg = 0.5 we achieved average DR = 0.48, 0.68 and 0.9 at SL = 1, 3 and 5 respectively. The ROC curve is not useful in determining the optimal operation point of MSDAR. On the contrary, the optimal operation point for each stage is declared by the CID curve shown in Fig. 12. Table V shows the maximum CID Levels corresponding to different parameters. It can be deduced that the performance of MSDAR improves by using multiple stages of different detection mechanisms.

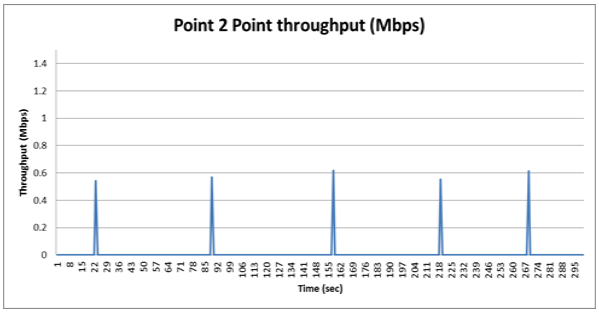


Fig. 8. Point to Point Throughput of the Simulated Network as measured by MSDAR

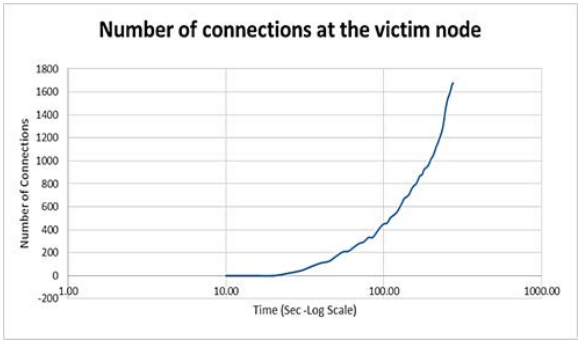


Fig. 9. Number of Connections at the Victim Node as measured by MSDAR.

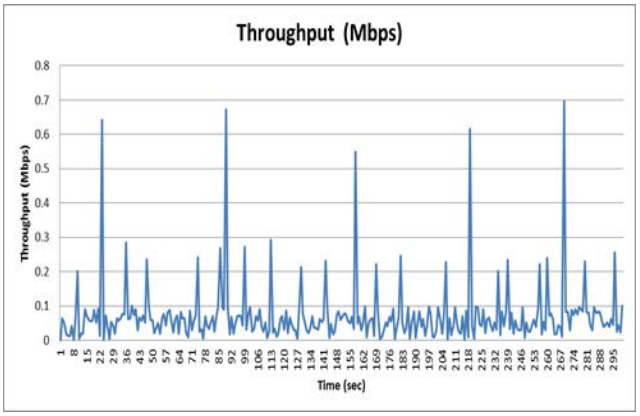


Fig. 10. Average Throughput of the Simulated Network as measured by MSDAR.

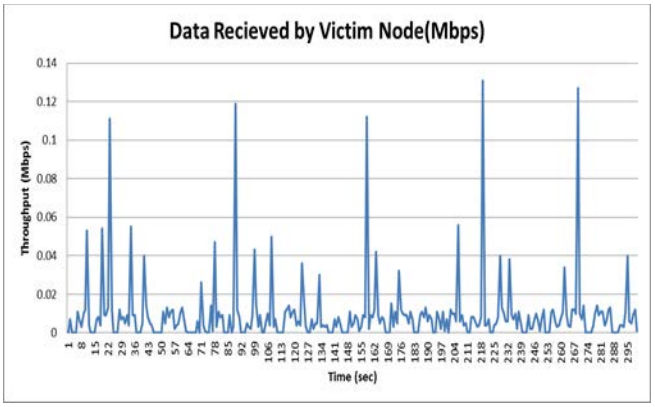
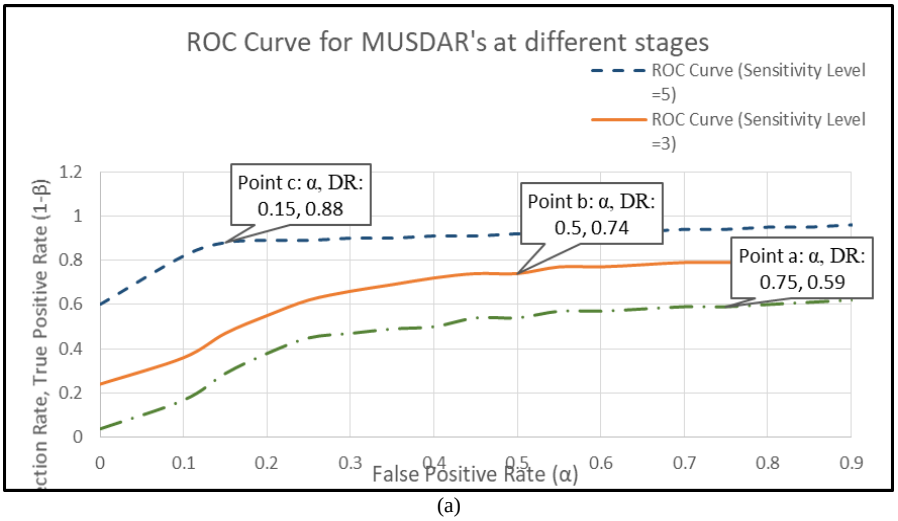


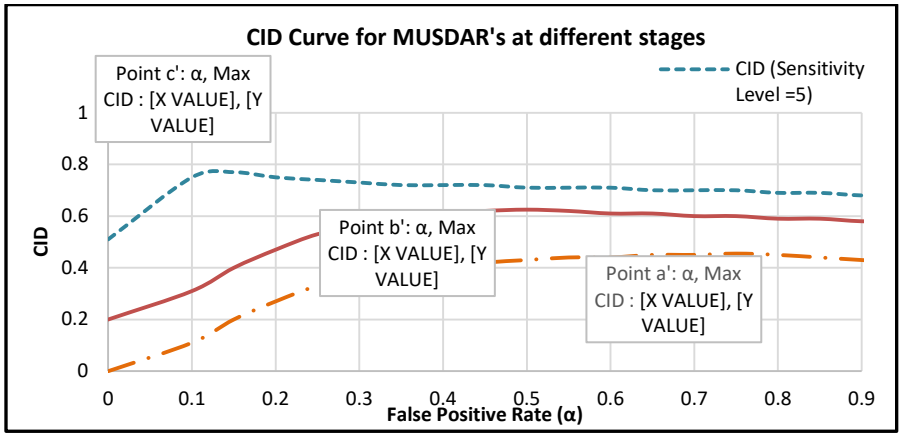
Fig. 11. Data Received by the Victim Node as measured by MSDAR.

TABLE V. MAXIMUM CID LEVELS CORRESPONDING TO DIFFERENT PARAMETERS

Point	α	SL	Maximum CID Level
a'	0.75	1	0.455
b'	0.5	3	0.625
c'	0.15	5	0.77



(a)



(b)

Fig. 12. MSDAR ROC Curve and its Corresponding Capability of Intrusion Detection (CID).

V. Discussion and Limitations

Our newly developed Multi Stage Dynamic Architecture (MSDAR) was explained in detail from the points of view architecture, sequence diagram, and flow chart. It was tested against DDoS attacks through simulations. Each event that scores greater than the predefined threshold is marked as an intrusion. Subsequently, a proper action using the MSDAR response mechanism is initiated. An important factor in evaluating the effectiveness of our proposed system was its ability to distinguish between intrusive and non-intrusive activities, with minimum false alarms. Results have shown that by increasing the IDS sensitivity level, the detection rate increases. The optimal operation point for each stage is declared by the CID curve. This research can be extended by using the statistical test (t-test/p-test/ANOVA to compare and benchmark our method with others. Machine learning models have been used for intrusion detection for over a decade [40]. We plan to use machine learning in one of the stages of our multistage Intrusion detection system MSDAR [41]. We will also use the model from [42] to assess the effectiveness of our suggested approach using machine learning.

VI. Conclusion and Future Work

Despite the various applications of Mobile Ad Hoc Networks, security challenges need to be addressed for both internal and external attacks. Intrusion detection systems are regarded as the second line of security against many types of attacks. Due to MANETs' special characteristics, traditional Intrusion detection systems cannot be used. In this paper, we distinguished between the different approaches used for intrusion detection mechanisms in a structured way. We classified intrusion detection systems with respect to different categories, such as architectures and design parameters. We introduced a standardized building block for intrusion detection systems for MANETs that summarizes different classifications of IDS techniques. In addition, a survey that shows the most popular design parameters used in different IDSs was presented. We proposed a multi-stage intrusion detection system (MSDAR) which is featured by its dynamic architecture as it can be deployed in the network using the Distributed Hierarchical Architecture (DHA-IDS), as it can dynamically change its deployment architecture. Simulations have shown that in case of an attack directed to the response mechanism unit, one of the cluster head analysis units is responsible for replacing the response mechanism unit. Similarly, in case the attack is extended to the cluster heads, each node depends on its data and makes its own decision regarding any suspected action.

Therefore, the proposed MSDAR can perform in the worst attack conditions and it can modify its architectural level from Distributed Hierarchical to Standalone, in order to retain the system's self-robustness. Furthermore, the new proposed architecture is capable of incapacitating many disadvantages of different architectures like; bottleneck congestion, single point of failure, processing, and power overhead. The suggested system's MSDAR effectively lowers false positives, increasing the intrusion detection system's capability and detection rate (CID) are increased by using the multi-stage feature. By measuring the CID level and comparing it to the detection rate, we were able to determine the optimal operation point for each stage in the proposed system. As a result, the total detection rate rises, increasing the network's functional efficiency to a tolerable level. In future work, MSDAR can be tested for different types of attack scenarios.

References

[1] Ahmed I, Jeon G, Piccialli F. From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where. IEEE Transactions on Industrial Informatics. 2022 Jan 27;18(8):5031-42.

[2] A. Nasir A, Shaukat K, Khan KI, Hameed IA, Alam TM, Luo S. What is core and what future holds for blockchain technologies and cryptocurrencies: A bibliometric analysis. IEEE Access. 2020 Dec 23;9:989-1004.

[3] Shaukat K, Alam TM, Hameed IA, Khan WA, Abbas N, Luo S. A review on security challenges in internet of things (IoT). In2021 26th International Conference on Automation and Computing (ICAC) 2021 Sep 2 (pp. 1-6). IEEE.

[4] Shaukat K, Iqbal F, Hameed IA, Hassan MU, Luo S, Hassan R, Younas A, Ali S, Adeem G, Rubab A, Iqbal R. MAC protocols 802.11: A comparative study of throughput analysis and improved LEACH. In2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) 2020 Jun 24 (pp. 421-426). IEEE.

[5] Pamarthi S, Narmadha R. Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile

Adhoc Networks for IoT Applications. Wireless Personal Communications. 2022 May;124(1):349-76.

[6] Ebazadeh Y, Fotohi R. A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold. Security and Privacy. 2022 Jan;5(1):e183.

[7] Ganesh SS, Ravi G. A stable link connectivity-based data communication through neighbour node using traffic-less path in MANET. International Journal of Vehicle Information and Communication Systems. 2020;5(1):72-89.

[8] M. G. El-Hadidi and M. A. Azer, "Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs," 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), 2021, pp. 155-160, doi: 10.1109/MIUCC52538.2021.9447611.

[9] M. A. Azer, N. G. Saad, “Prevention of Multiple Coordinated Jellyfish Attacks in Mobile Ad Hoc Networks” International Journal of Computer Applications. 2015 Jan 1;120(20).

[10] Hemalatha S, Kshirsagar PR, Manoharan H, Vasantha Gowri N, Vani A, Qaiyum S, Vijayakumar P, Tirth V, Haleem SL, Chakrabarti P, Teressa DM. Novel Link Establishment Communication Scheme against Selfish Attack Using Node Reward with Trust Level Evaluation Algorithm in MANET. Wireless Communications and Mobile Computing. 2022 May 6;2022.

[11] Bondada P, Samanta D, Kaur M, Lee HN. Data Security-Based Routing in MANETs Using Key Management Mechanism. Applied Sciences. 2022 Jan;12(3):1041.

[12] Almalki FA, Soufiene BO. EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. Wireless Communications and Mobile Computing. 2021 Mar 9;2021.

[13] Sultana T, Mohammad AA, Gupta N. Importance of the Considering Bottleneck Intermediate Node During the Intrusion Detection in MANET. In Research in Intelligent and Computing in Engineering 2021 (pp. 205-213). Springer.

[14] Shaukat K, Alam TM, Luo S, Shabbir S, Hameed IA, Li J, Abbas SK, Javed U. A review of time-series anomaly detection techniques: A step to future perspectives. In Future of Information and Communication Conference 2021 Apr 29 (pp. 865-877). Springer, Cham.

[15] Kumar S, Dutta K. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. Security and Communication Networks. 2016 Sep 25;9(14):2484-556.

[16] Singh S, Sharma S, Sharma S, Alfarraj O, Yoon B, Tolba A. Intrusion Detection System based Security Mechanism for Vehicular ad-hoc Networks for Industrial IoT. IEEE Consumer Electronics Magazine. 2021 Dec 28.

[17] Khan K, Mehmood A, Khan S, Khan MA, Iqbal Z, Mashwani WK. A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture. 2020 May 1;105:101701.

[18] Li W, Meng W, Kwok LF. Surveying Trust-based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions. IEEE Communications Surveys & Tutorials. 2021 Dec 28.

[19] Ramesh S, Yaashuwanth C, Prathibanandhi K, Basha AR, Jayasankar T. An optimized deep neural network based DoS attack detection in wireless video sensor network. Journal of Ambient Intelligence and Humanized Computing. 2021 Jan 2:1-4.

[20] Marathe NR, Shinde SK. Improved itca method to mitigate network-layer attack in manet. InData Communication and Networks 2020 (pp. 245-253). Springer, Singapore.

[21] Sinha S, Paul A. Neuro-fuzzy based intrusion detection system for wireless sensor network. Wireless Personal Communications. 2020 Sep;114(1):835-51.

[22] S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, L.T. Heberlein, C.L. Ho, K.N. Levitt, "DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype". In Proceedings of the 14th national computer security conference 1991 (Vol. 1, pp. 167-176).

[23] F. Cuppens, and A. Miege, "Alert correlation in a cooperative intrusion detection framework". In Security and privacy, 2002. Proceedings. 2002 IEEE symposium on (pp. 202-215). IEEE.

[24] P. Kannadiga, and M. Zulkernine, "DIDMA: A distributed intrusion detection system using mobile agents". In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2005 (pp. 238-245). IEEE.

[25] Staniford-Chen S, Cheung S, Crawford R, Dilger M, Frank J, Hoagland J, Levitt K, Wee C, Yip R, Zerkle D. GrIDS-a graph based intrusion detection system for large networks. InProceedings of the 19th national information systems security conference 1996 Oct 22 (Vol. 1, pp. 361-370).

[26] Zhang Z, Li J, Manikopoulos CN, Jorgenson J, Ucles J. HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. InProc. IEEE Workshop on Information Assurance and Security 2001 Jun 5 (pp. 85-90).

[27] Axelsson S. Intrusion detection systems: A survey and taxonomy. Technical report; 2000 Mar 14.

[28] Janakiraman R, Waldvogel M, Zhang Q. Indra: A peer-to-peer approach to network intrusion detection and prevention. In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on 2003 Jun 9 (pp. 226-231). IEEE.

[29] Zhou, C.V., Karunasekera, S. and Leckie, C., 2007, May. Evaluation of a decentralized architecture for large-scale collaborative intrusion detection. In Integrated Network Management, 2007. IM'07. 10th IFIP/IEEE International Symposium on (pp. 80-89). IEEE.

[30] M. Raya, J.P. Hubaux, and I. Aad, " DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In Proceedings of the 2nd international conference on Mobile systems, applications, and services 2004, (pp. 84-97). ACM.

[31] M. Roesch, "Snort: Lightweight intrusion detection for networks. In Lisa 1999 (Vol. 99, No. 1, pp. 229-238).

[32] Fung CJ. Collaborative Intrusion Detection Networks and Insider Attacks. JoWUA. 2011 Mar;2(1):63-74.

[33] Kruegel, C., Toth, T., Kerer, C.: Decentralized Event Correlation for Intrusion Detection. In: International Conference on Information Security and Cryptology (2002).

[34] Maciá-Pérez F, Mora-Gimeno FJ, Marcos-Jorquera D, Gil-Martínez-Abarca JA, Ramos-Morillo H, Lorenzo-Fonseca I. Network intrusion detection system embedded on a smart sensor. IEEE Transactions on Industrial Electronics. 2011 Mar;58(3):722-32.

[35] Albers P, Camp O, Percher JM, Jouga B, Me L, Puttini RS. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In Wireless Information Systems 2002 Apr 3 (pp. 1-12).

[36] Gu G, Fogla P, Dagon D, Lee W, Skorić B. Measuring intrusion detection capability: an information-theoretic approach. In Proceedings of the 2006 ACM Symposium on Information, computer and communications security 2006 Mar 21 (pp. 90-101). ACM.

[37] Kumar G. Evaluation metrics for intrusion detection systems-a study. International Journal of Computer Science and Mobile Applications, II. 2014 Nov.

[38] F. Alam TM, Shaukat K, Hameed IA, Khan WA, Sarwar MU, Iqbal F, Luo S. A novel framework for prognostic factors identification of malignant mesothelioma through association rule mining. Biomedical Signal Processing and Control. 2021 Jul 1;68:102726.

[39] MIT Lincoln Laboratory: DARPA Intrusion Detection Evaluation, https://www.ll.mit.edu/ideval/data/2000data.html.

[40] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in IEEE Access, vol. 8, pp. 222310-222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[41] Shaukat K, Luo S, Varadharajan V, Hameed IA, Chen S, Liu D, Li J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies. 2020 Jan;13(10):2509.

[42] Shaukat K, Luo S, Chen S, Liu D. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In2020 International Conference on Cyber Warfare and Security (ICCWS) 2020 Oct 20 (pp. 1-6). IEEE.