Research Article

A Torpor-based Enhanced Security Model for CSMA/CA Protocol in Wireless Networks

Abiodun Akinwale, John E. Efiong, Emmanuel A. Olajubu* and Ganiyu A. Aderounmu
Obafemi Awolowo University, Nigeria
logitronics@yahoo.com; jeediof@gmail.com; emmolajubu@oauife.edu.ng; gaderoun@oauife.edu.ng
*Correspondence: emmolajubu@oauife.edu.ng

Received: 12th April 2023; Accepted: 30th March 2024; Published: 1st April 2024

Abstract: Mobile wireless networks enable the connection of devices to a network with minimal or no infrastructure. This comes with the advantages of ease and cost-effectiveness, thus largely popularizing the network. Notwithstanding these merits, the open physical media, infrastructural-less attributes, and pervasive deployment of wireless networks make the channel of communication (media access) vulnerable to attacks such as traffic analysis, monitoring, and jamming. This study designed a virtual local area network (VLAN) model to circumvent virtual jamming attacks and other intrusions at the Media Access Control (MAC) layer of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. A Torpor VLAN (TVLAN) Data Frame Encapsulation and the algorithm for T-VLAN security in CSMA/CA were formulated and presented. A simulation experiment was conducted on the model using OMNeT++ software. The performance metrics used to evaluate the model were packet delivery ratio, network throughput, end-to-end channel delay, and channel load. The simulation results show that the TVLAN defence mechanism did not increase the channel load arbitrarily during TVLAN defence. similarly, the system throughput was shown to be 82% during TVLAN defence. Nevertheless, the network delay of the system during TVLAN defence was significantly high but the channel load was 297 when the TVLAN security mechanism was launched. These results demonstrate the model's ability to provide a survivability mechanism for critical systems when under attack and add a security layer to the CSMA/CA protocol in wireless networks. Such a remarkable performance is required of a CSMA/CA infrastructure for improving the cybersecurity posture of a wireless network.

Keywords: *IoT; IP; MAC address; MANET; Torpor VLAN; TVLAN*

1. Introduction

Wireless networks generally refer to networks connected by radio waves for communication between participating network nodes. Some types of networks allow devices to be connected to the network while roaming around within the network coverage only, while others use multi-hop attributes to connect to the network when outside its range using a nearby intermediate node that is within the network range. Examples of such networks include Wireless sensor networks (WSN), Ad hoc Street light networks (ASLN), Mobile ad hoc networks (MANET), and the Internet of Things (IoT) [1].

WSNs are data logging systems where autonomous spatially distributed computing nodes with sensors work together to monitor environmental information and to cooperatively forward data to central servers in homes and industries as cyber-physical systems. An ad hoc street light network involves the use of wireless internet protocol (IP) signals to monitor and control street lights for efficiency and maintenance. Single systems can then remotely control thousands of such lights, detect faulty ones, and adapt them to the ambient temperature and illumination for efficiency and longevity. A MANET-the focus of this work-is an autonomous network formed spontaneously or semi-permanently without any established

Abiodun Akinwale, John E. Efiong, Emmanuel Olajubu and Ganiyu Aderounmu, "A Torpor-Based Enhanced Security Model for CSMA/CA Protocol in Wireless Networks", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 43-55, Vol. 8, No. 2, 1st April 2024, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2024.02.004, Available: http://aetic.theiaer.org/archive/v8/v8n2/p4.html.

infrastructure or centralized administration [1]. The network consists of mobile nodes that are integrated hosts and routers, equipped with a wireless interface. The spontaneity, topology independence, and zero requirements for fixed infrastructure have made this type of network very useful to many application areas. IoT networks are modified WSNs for domestic, office, and social usage whereby virtually any common appliance can be embedded with sensors and minute processors that connect to the internet. MANETs are now also being deployed to critical areas such as disaster relief situations, law enforcement, public meetings, virtual classrooms, commerce, and other security-sensitive plus mission-critical computing environments [1]. There are MANETs dedicated to solving specific problems like vehicular ad hoc networks (VANETs) and unmanned aerial networks (UAVs). These are mainly used for communication among land-based and aerial vehicles respectively and between vehicles and roadside equipment or control towers respectively [2]. According to [3] the development of new hardware such as smart vehicles, intelligent drones as well as new software for embedded platforms incorporating internet-of-things (IoT) are benefits of wireless systems used for smart homes and industries. WSNs are now being widely used in factories and robot-controlled automation processes.

The media access control (MAC) of a network is embedded in the first layer of the TCP/IP protocol and it defines access to a wireless channel intended for deployment of a contention-free experience that maximizes channel utilization [1]. According to Kumar and Dutta in [4], the two MAC protocols mostly used are contention-free and contention-based algorithms. Contention-free schemes use an assignment of time and frequency to allocate shared media which is collision-free [5]. In Contention-based schemes, the entire channel is open for the nodes to compete or "contend" to access the medium. For example, in Carrier Sense Multiple Access (CSMA), the node defers transmission when it senses other nodes in the network are transmitting to avoid collision. Wireless systems use a collision avoidance scheme named carrier sense multiple access with collision avoidance or CSMA/CA. The focus of this work is the CSMA/CA protocol which is widely used in 802.11(fixed and mobile wireless), 802.11p (vehicle ad hoc), and 802.15.4 (sensor/IoT) standards for wireless networks.

The open physical media, infrastructural-less attributes, and pervasive deployment of wireless networks make the channel of communication (media access) vulnerable to attacks such as traffic analysis, monitoring, and jamming. Jamming at the MAC sub-layer is known as virtual jamming as opposed to physical (radio) jamming that takes place at the physical sub-layer of the TCP/IP protocol suite. A lot of research has been done to secure wireless networks but most of these models focus on the upper layers of the TCP/IP protocol, especially on the routing layer. However, the routing layer depends largely on the input from the physical and MAC sub-layers of the first (network access) layer. Existing works on CSMA/CA security are few and are tailored to detecting or protecting a specific segment of the CSMA/CA protocol algorithm while leaving the other areas unprotected and in need of another procedure for detection and protection. Using extra defence procedures increases the processor and energy overheads for a network having limited resources, this is unacceptable. The need to secure the entire CSMA/CA protocol against diverse attacks (novel or known), using a simple procedure that will not consume many node/network resources form the basis for this work. Our proposed torpor model confers a capability on CSMA/CA-based networks to reduce non-essential activities to conserve system resources and maintain acceptable performance for mission-critical processes in the face of inclement network conditions and intrusion. The network enters the torpor state in short bursts or prolonged periods as network conditions dictate. The proposed model shows that in most tightly contested network scenarios, a trade-off of reducing non-essential processes leads to significant system survivability. The next segment of this paper discusses related work in this area; section 3 presents our theory and the basis of this work, and section 4 discusses the method employed for this work. The next section is the experimental work for the study while section six presents the simulation results of the experiment. Section seven concludes the paper.

2. Related Works

There are several studies [6 - 11] in the literature seeking how to effectively tackle jamming attacks on wireless networks. In recent times, a jamming detection attack [12] was designed based on machine learning algorithms for vehicular networks [13]. Study [12] investigated the use of hidden rules and how it affects the observation changes under a reactive jamming attack while the latter classified the different jamming attacks based on the techniques employed by the attackers [14]. The two models' performances were good but synthetic data were used, and the analysis of correlation or deviation from existing standard data for such an experiment was not presented. From a different perspective, while seeking an accurate solution to a jamming attack that is capable of disrupting and disabling wireless networks [15] analysed the use of deep learning algorithms for detecting jamming and interference attacks with a view of developing a robust query-based method for effective mitigation. The model explores the relationship that exists within the same node with those parameters of the neighbouring nodes on the network as done by [16]. When abnormal parameters are viewed correlation is done with the neighbouring nodes, if there is a significant differential, a packet query is issued which analyses the queried packet, the variation is used to suspect an attack, and immediately attack flag attack is immediately raised. A mitigation process is initiated to resolve the attack.

In similar research, [17] designed a model to evaluate different types of jamming attacks on a wireless network. There are four modules of classes designed in the work. Physical Layer Driver Class was designed to connect the jamming with the WiFi-Phy so that the physical layer of WiFi can be simulated using NS-3 simulation software. A jammer class was introduced to allow different jamming techniques to be implemented. A jamming mitigation class was implemented to handle any type of jamming attack and a wireless utility class provides connection among the different modules of the system. Packet delivery ratio (PDR) is used as the main metric for the work. The result showed that during mitigation, PDR was 0% and during mitigation, it varies between 60% and 70%. A k-tuple Full Withholding (KTFW) algorithm was proposed for CSMA/CA in [18] to increase the resilience of MAC against jamming attacks. The algorithm is meant for an environment where nodes are not allowed to add extra information to the packet and the nodes are listening for feedback on the channel continuously. The algorithm was compared with binary exponential backoff and queue backoff which were algorithms used to mitigate jamming and found out that the proposed algorithm showed great throughput and less average packet delay when mitigating jamming attacks. A process decision-making model based on the Markov chain with a contention window was designed in [19] for CSMA/CA to resolve jamming attacks on wireless networks. In this model, backoff was used as the control variable while throughput was the reward value. Each node on the network was equipped with a transmitter and a receiver which employed half-duplex communication mode with other nodes. The nodes used distributed learning decision-making to query the status collection equipment. The anti-jamming process was improved through learning and adapting to the environment. When simulated within 10 nodes, in a non-jamming environment, the throughput was increased by 28%, in an intermittent jamming environment the throughput was increased by 21.2 0% while in a random jamming environment the throughput was increased by 17.07%, which shows that even in the face on an attack, the performance of the network rarely dwindles.

In a similar scenario, jamming attack detection was conducted in [20] to examine the reactive jamming attack. A framework for reactive jamming detection using radio frequency sensors outside of the network was developed. Underdetermined blind source separation was able to separate the jamming temporal file from network nodes' broadcasting profiles and all-versus-one transfer entropy was used to design new jamming attack detection. When applied to the network, a 90% probability of detection was achieved with 6% of false alarms. The collaborative jamming attack was investigated on the Internet of Things (IoT) in [21 -23]. The attackers used prior knowledge of the network and the limitations of IoT to penetrate and launch the jamming attack. The attackers form a coalition through an exchange of information using probability-connected three windows to select the node to attack. The model employed a look-up table which is regularly updated to break the coalition and free the network from the attack.

The proposed model empowers the CSMA/CA-based networks to curtail activities that are not major to the mission of the system to preserve system resources and provide acceptable performance for mission-critical systems in the presence of network attacks and intrusion. The network assumes the inertia state in a short period or prolonged time depending on the network condition. The proposed model shows that in a presence attack, the trade-off of reducing non-essential processes leads to significant survivability of the system. Our concern is that a mission-critical system should still be able to continue to deliver or serve the users even when under attack.

3. Theoretical Framework

3.1. Formulation of Torpor Mathematical Model

For this work, the state of torpor is described as a hypo activity network state where non-critical network activities are reduced or saved to achieve optimum survivability. The inspiration for the model was derived from the [24] that demonstrated how living organisms can redistribute energy to achieve optimum performance. Living organism normally minimizes their metabolic activities to conserve energy during unwholesome times. The energy saved during the period is channelled to survivability which assists such animals to survive challenging periods such as dry seasons. The model also employed Kirchhoff's 1st law and Schmidt's theory of energy allocation to design a survivability defence mechanism for CSMA/CA protocol in mobile wireless networks. Kirchoff's first law, which is also known as the law of conservation of current, is used to model total network resources or total flow of data in MANETs. The law states that the total current flowing into a junction or node in the network must be equal to the total current flowing out of the node. This principle is used to model the flow of data in the network to ensure equilibrium, efficiency, and security.

Applying Kirchoff's first law, we have the following equation:

$$\sum d_{in} = \sum d_{out} \tag{1}$$

Where: $\sum d_{in}$ represents the total resources or data flow from a mobile network to nodes, and $\sum d_{out}$ represents the total outgoing data flow from a node to the network. Adapting Schmidt's theory [x] that the allocation of energy to the different functions of an organism is determined by its life history strategy and its ecological environment, the function of resource allocation to enhance network survivability during attacks is explored for wireless networks' security. Schmidt's energy allocation function postulates that repartitioning of metabolic operations leads to optimum performance. Applying the mathematical model of Schmidt's theory to mobile computer networks, resources are reallocated to different network functions during an attack. While bandwidth resources are reduced for maintenance (channel and signal) and mobility, more resources are committed to data transfer and security or defence. The gain from reduced allocations offsets the cost of more resources for security and data transfer. Let total network resources or bandwidth be represented by the symbol B. The bandwidth allocated to data transfer, maintenance, security, and Node mobility is denoted as T, M, S, and N respectively. Relying on Schmidt's theory, the allocation of bandwidth to these different functions is determined by the network's size and attack scenarios. This model can be represented by the following equation:

$$B = T + M + S + N \tag{2}$$

This equation states that the total bandwidth available B during an attack must be equal to the bandwidth allocated to data transfer T, maintenance M, security S, and node mobility N combined. To achieve survivability and optimize network performance, there is the need to allocate bandwidth resources to the network for maximum security and efficiency. The model for the allocation is presented in equation (2). The network security and efficiency are denoted as S and E respectively, and it is assumed that the network security or defence is a function of the bandwidth or network resources allocated to data transfer T, which is also denoted as T. The T-VLAN defence mechanism is presented in Figure 1, where S is the maximum security in the face of diverse attack scenarios. Then this defence mechanism is expressed as equations (3) and (4) respectively subject to equation (2):

$$maximize\ S = f(T) \tag{3}$$

The above optimization expression is to maximize the network security S subject to the constraint of the total available bandwidth B and must be re-allocated to data transfer, maintenance, and security T, M, S, and N during an attack. While bandwidth resources are reduced for maintenance (channel and signal) and mobility, more resources are committed to data transfer and security or defence. Solving the above problem by reallocating network resource functions to maximize network security and efficiency gives the optimum security required. The solution, as stated earlier, depends on network size and attack scenario or environment resources. To solve this optimization problem in equation (3) and achieve maximum security, the method of Lagrange multipliers was adopted. The Lagrangian function for this problem is written as equation (4):

$$L(T, M, S, \lambda) = f(T) + \lambda(B - T - M - S) \quad (4)$$

Where: λ is the Lagrange multiplier.

To find the optimal solution in equation (4), the partial derivatives of L with respect to T, M, S, and λ, were taken and set equal to zero as shown in equations (5)-(8):

$$\frac{\partial L}{\partial T} = f(T) - \lambda = 0 \quad (5)$$

$$\frac{\partial L}{\partial M} = -\lambda = 0 \quad (6)$$

$$\frac{\partial L}{\partial S} = -\lambda = 0 \quad (7)$$

$$\frac{\partial L}{\partial \lambda} = B - T - M - S - N = 0 \quad (8)$$

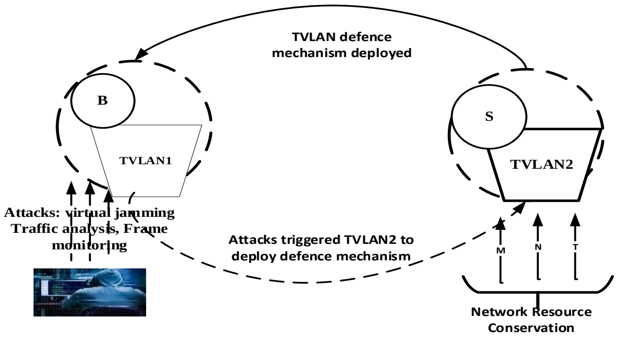


Figure 1. TVLAN Defence Mechanism Deployment

From (5), the marginal benefit shown in equation (9) is calculated thus:

$$f'(T) = \lambda \quad (9)$$

This means that the marginal benefit of allocating an additional unit of bandwidth to data transfer is equal to the Lagrange multiplier λ, from equations (8), (7) and (9), $\lambda = 0$.

It is implied in equation (10) that the Lagrange multiplier λ is zero, indicating that there are no constraints on the optimal solution, and the total allocated bandwidth (T + M + S) must equal the total available bandwidth (B) which satisfied the Kirchhoff's Law of conservation of energy. From the first equation, we get:

$$f'(T) = 0 \quad (10)$$

This means that during an attack, the optimal security solution occurs at the point where the marginal benefit of allocating an additional unit of bandwidth to security is zero. Therefore, the optimal reallocation of network resources or bandwidth during an attack can be found by maximizing the network defence subject to the constraint that the total allocated bandwidth must equal the total available bandwidth.

A summary of network parameters used are as follows:

a. Total network resource or bandwidth is total network resources at the normal state before attack = B
b. The cost of torpor operations defence or security is the resource cost of deploying torpor defence = S
c. Maintenance frames are frames used to maintain channel access as well as signal broadcast = M
d. Node Mobility is the basic attribute of mobile nodes to move = N
e. Data transfer or throughput = T

3.2. CSMA/CA Protocol Operation

The basic CSMA/CA algorithm is presented as follows:

a. Before a frame transmits data, the sender inspects the network channel, to know if the channel is busy or free.
b. If the channel flags busy mode, data transmission is kept back till the channel becomes idle using the persistence algorithm to check the channel.
c. If the channel flags idle mode, the node waits for the distributed coordination function inter-frame space (DIFS) for an amount of time and then sends a request to send (RTS) control message to the receiver. The timer is set. When a clear-to-send (CTS) message is received before

timeout, it then waits for short inter-frame space (SIFS) time and sends the frame (otherwise it increments back-off time). If the back-off time is exceeded, abort the operation. If not, go to step (a) above)

d. A timer is set after sending the frame.

e. The node that transmits data then waits for ACK (acknowledgment) from the destination node. If the ACK is received before the expiry of the timer, then there is successful transmission.

f. Otherwise, the node waits for a back-off time and restarts as in step (a) above.

3.3. Vulnerabilities of CSMA/CA Protocol and IDS Deployment

CSMA/CA has become a target of many attacks because it is one of the most popular data link layer protocols for wireless networks. For system survivability, the torpor model is deployed at vulnerable points in the protocol and is put under continual surveillance. These points are the (SIFS) observance, the (DIFS), and the (ACK) reply protocol sequence. Handshake times- (RTS) and (CTS) are not treated specially, since they use SIFS times. A jamming attack, for example, violates the SIFS or DIFS protocol-constrained timing by flooding the channel with unauthorized frames. These vulnerable points are explored by intruders for cheap attacks and gaining access to CSMA/CA protocol. Signature-based Intrusion detection systems (IDS) are then deployed to the above vulnerable points.

4. Methodology

Our proposed torpor model employs Schmidt's theory of network reallocation using the technique of network fragmentation and aggregation for survivability against attacks. Network fragmentation is used once an attack is detected. A counter monitors when an intrusion has been nullified and network fragments are aggregated to become a single entity as the original network thus network equilibrium is preserved. A VLAN is a technology that divides a physical local network into two or more virtual networks through software methods without physically rearranging the nodes. This attribute is explored for security enhancement in this work. This implies that to achieve defence in the face of attack, the broadcast domain is reduced through the fragmentation of the network into two or more VLANs as shown in Figure 1 shown previously. The bandwidth or network resource gained due to a reduced broadcast chain is reallocated for defence activities.

The torpor-VLAN or TVLAN technique ensures that at the point of fragmentation, current sending and receiving nodes are partitioned to the same VLAN to prevent data frame loss. Although VLAN technology is mostly used for wired ethernet networks, the concept is used in this work by integrating the IEEE802.1q standard into wireless CSMS/CA protocol for mobile devices. Figure 2 shows a TVLAN frame.

4.1 TVLAN Membership

TVLAN membership is determined by inserting the VLAN TAG -which includes VLAN ID (VID)- into the control frames of the anode at the point of entry into the ad hoc network. By default, all network nodes belong to the same broadcast domain or the default VLAN ID.

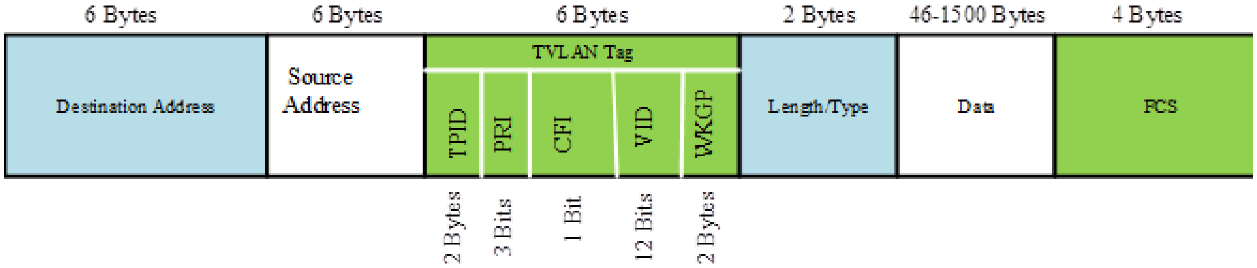


Figure 2. Proposed T-VLAN Data Frame Encapsulation

There are five distinct fields found in the TVLAN data frame Tag, they are TPID (Tag Protocol Identifier), PRI (Priority), CFI (Canonical Format Indicator, standard format indicator), and VID. The word length of TPID is 16 bits, and its main purpose is to ascertain the data frame contains a VLAN tag, and the value is 0x8100. The 802.1P indicates the priority of the communication with a length of 3 bits. The CFI field's main usefulness is to predetermine whether the MAC address is captured following the normal standard in another transmission channel. It is 1 bit in length and the value is either 1 or 0 which is the default value, 0 implies the MAC address is captured in the standard format, and 1 implies that it is captured in a non-standard format. VID determines the number of VLAN that has a particular message, it has a length of 12 bits. The content ranges from 0 to 4095, in as much as 0 and 4095 are the protocol reserved values the message content of the VLAN ID is between 1 to 4094.WKGP identifies the workgroup the node belongs to. This field denotes the description and ID number of the broadcast domain.

4.2. Proposed Technique

All nodes joining the network must have their frame header modified to include a VLAN tag by incorporating IEEE 802.1Q standard at the point of authentication for network access. The VLAN tag has an extra field called workgroup ID (WKRG) to accommodate the different workgroups of all participating nodes. Initially, all nodes are then set to the default VLAN ID which is 1. The entire algorithm is shown in Figure 3. Once an intrusion is detected by signature-based IDS, the TVLAN defence mechanism of network resources reallocation is activated. The first step checks the transmission state of the network by identifying the MAC addresses of currently transmitting and receiving nodes and that of the attacker. Secondly, the instantaneous size of the network as well as the number of workgroups are then recorded. For step three, The BLOCK INTRUDER process (to block the offending node) is triggered to block the MAC address of the attacker.

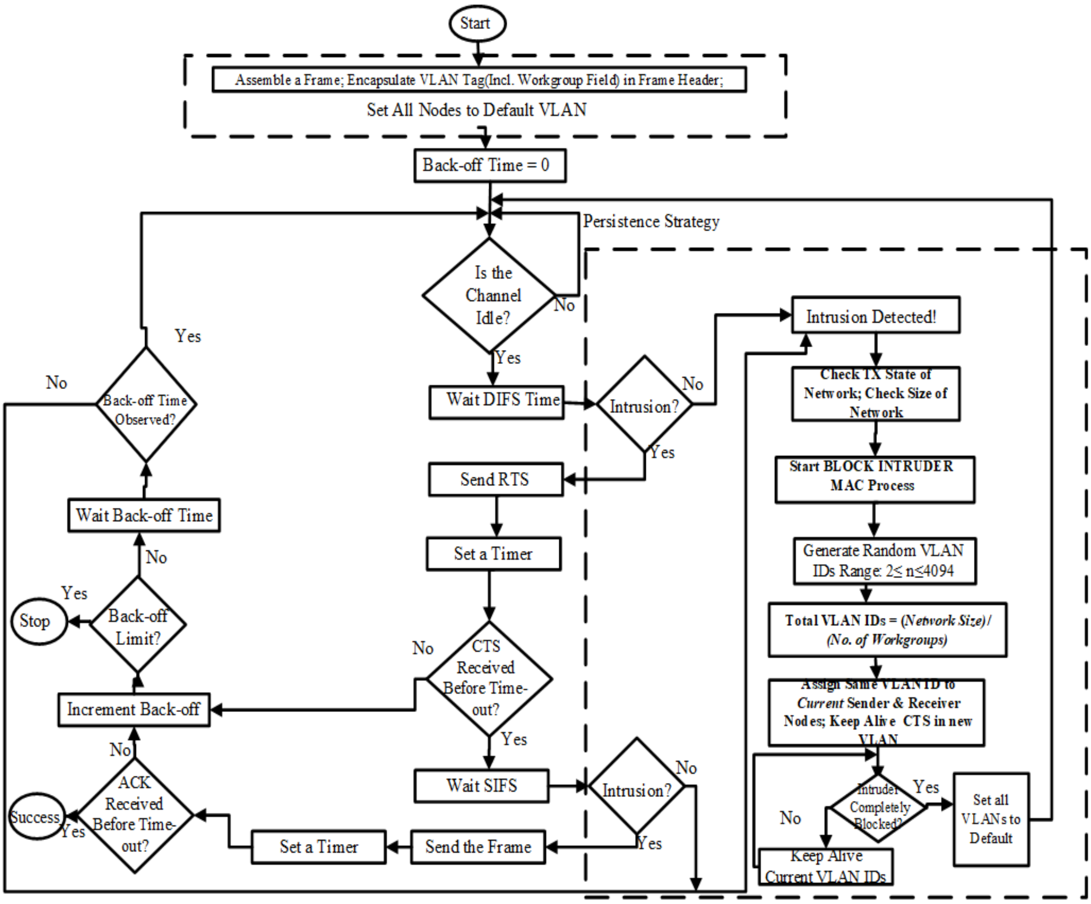

Start
Assemble a Frame; Encapsulate VLAN Tag(Incl. Workgroup Field) in Frame Header;
Set All Nodes to Default VLAN
Back-off Time = 0
Persistence Strategy
Is the Channel Idle?
No
Yes
Wait DIFS Time
Intrusion?
No
Yes
Send RTS
Set a Timer
CTS Received Before Time-out?
No
Yes
Wait SIFS
Intrusion?
No
Yes
Send the Frame
Set a Timer
ACK Received Before Time-out?
Yes
Success
No
Increment Back-off
Back-off Limit?
Yes
Stop
No
Wait Back-off Time
Back-off Time Observed?
Yes
No
Intrusion Detected!
Check TX State of Network; Check Size of Network
Start BLOCK INTRUDER MAC Process
Generate Random VLAN IDs Range: 2≤ n≤4094
Total VLAN IDs = (Network Size)/ (No. of Workgroups)
Assign Same VLAN ID to Current Sender & Receiver Nodes; Keep Alive CTS in new VLAN
Intruder Completely Blocked?
Yes
No
Set all VLANs to Default
Keep Alive Current VLAN IDs

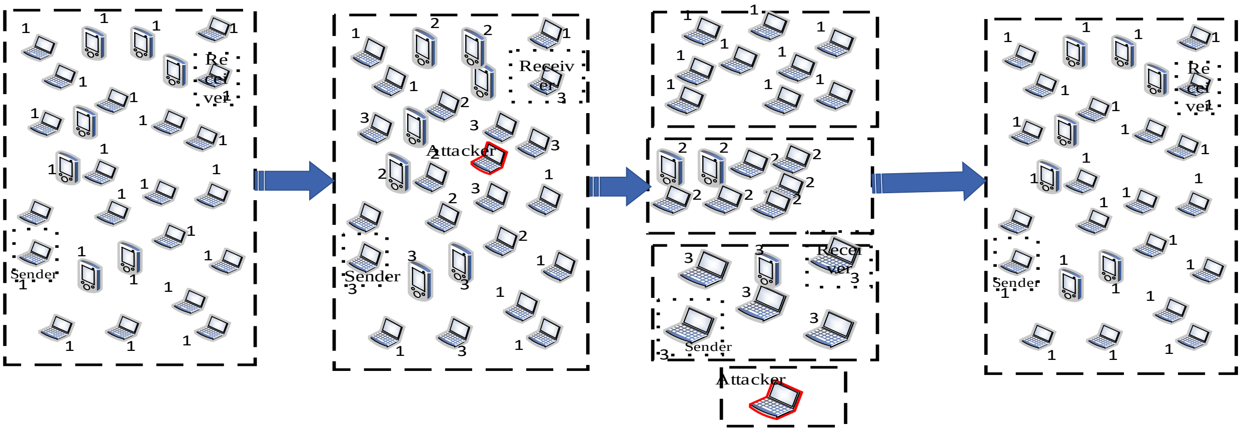
Figure 3. Algorithm for TVLAN security for CSMA/CA

TVLAN at this stage generates random VLAN IDs from 2 to 2094 for partitioning the network to smaller broadcast domains. The total number of VLAN IDs that will be used is the ratio of the current size of the network to the number of workgroups. If all nodes belong to just one workgroup, TVLAN uses Equation (11) below to calculate the total number of VLAN IDs.

$$No. of\ VLAN\ IDs = 2^n \quad (11)$$

where *n is the No. of bits borrowed*

Next, TVLAN randomly chooses a VLAN ID or VID and assigns the same to both the transmitting and receiving nodes. To ensure continuous data transfer, the current CTS control message already issued to the sender is kept alive in the new VLAN. After the above process, the system checks to know if the attacker has been completely blocked and isolated. This is subject to Equations (2) and (3) listed earlier for maximizing security. All VLANs are aggregated back to the default VLAN as shown in Figure 4 below, otherwise, current VLAN IDs are maintained until the blocking process is completed and VLANs are aggregated. All the above processes must take place in milliseconds subject to Equation (5), (6), (7) and (8).



Stage 1: Original Mobile Wireless Network with VLAN Tag and Workgroup Field in Frame Encapsulation (at Authentication); Default VLAN ID; current Sender and Receiver Nodes

Stage 2 : Attack Detected; TVLAN Activated; VLAN IDs Generated based on no. of Workgroups; Sender and Receiver given same VLAN ID; Data Transfer continues.

Stage 3: Network Fragmented to Multiple Workgroup VLANs; Attacker Isolated from Network and Blocked! Data Transfer Continues.

Stage 4: Aggregation of VLANs to become Original Single Network with Default VLAN ID; Data Transfer Continues.

Figure 4. TVLAN Fragmentation, Isolation, and Aggregation Process

5. Experimental Setups

OMNeT++ was the main tool used to determine the performance of the proposed torpor-based defence of the CSMA/CA protocol evaluated in this work. Written in C++, it is a suitable testbed for TVLAN simulation. Its inbuilt INET Framework module suite was used because of the vast set of models it possesses for mobile networks and the ability for a user to customize the output vector statistics to his requirements. In this section, simulation processes and parameters for CSMA/CA are discussed.

5.1 . OMNeT Simulation

In this work, three main classes of scenarios for CSMA/CA were modelled and simulated. The setup was used to model (i) a normal protocol (ii) The protocol under attack and (iii) The protocol with a TVLAN defence countermeasure. The parameters for the experimental setup in OMNET++ are shown in Table 1 below.

5.2. OMNeT Simulation Process

The network configuration, the deployment of the TVLAN defence module, and the simulation initialization were carried out in OMNeT++ using four main files namely the .cc (source code file), .h (header file), .ini ((initialization file) and. ned (interface description file). The .cc file contains the source code of the different processes. Each process is represented by a C++ class. The .h file is used for declaring classes and variables used in .cc file. For the configuration of the simulation interface, the type of nodes used, the network topology, and the placement of the nodes were specified in the .ned file. The medium used, the specification of the protocol or module being simulated and the configuration of simulation parameters (time, statistics recording) were done in the .ini file. The files were linked as follows: the classes and variables were declared in the .h file, and the contents of these classes were written in the .cc file which defined the module to be used by the .ned file. Finally, the .ini file calls the .ned file for initializing the simulation.

5.3 CSMA/CA Protocol

MANET is based on the IEEE 802.11 standards. The preeminent access sub-layer protocol h is the CSMA/CA which controls multiple access to the same channel. The algorithm for the protocol processes has been discussed already. In OMNET++ CSMA/CA is realised within the INET framework wireless LAN module. Internally, CSMA/CA captures packets with its headers and trailers at the source node, and it decapsulates packets at the destination node. The headers and trailers contain the information required to offer the protocol-specific service. When a packet is received, the CSMA/CA protocol takes away the header from the received frame and passes the resulting datagram along.

Table: 1. Simulation Parameters

Parameter	Value
Simulation Time	3600s
Number of Nodes	100
Simulation Area (m)	500X500
Sending Interval	0.1
Protocol	CSMA/CA
Node Speed (m/s)	10
Data Rate (Mb/s)	1Mbps
Transmit Power (W)	2.0mW
No of Channel	10
Carrier Frequency (Hz)	2.4/5GHz
Traffic Model	TCP
MAC Protocol	IEEE 802.11g
PacketSize – CBR (bytes)	10

5.4. OMNeT Performance Metrics for Evaluation

Performance metrics represent the whole characterization of an entire network or a particular node being studied. The metrics were used in the evaluation of the protocols simulated. In this study, four performance metrics used were: network load, packet delivery ratio, network throughput, and end-to-end delay.

5.5. Frame Load

This metric measures the amount of traffic generated during the discovery and maintenance processes of a protocol for example, the total number of RTS, CTS, and ACK datagrams in CSMA/CA protocol. Factors contributing to high overhead include: the size of the network- which leads to multiple hops from source to destination and the mobility rate- more links are made and broken arbitrarily when mobility increases. The lower the load or overhead is, the more efficient a protocol will be as calculated with equation (12).

$$Frame\ Load = Total\ No.of\ RTS + Total\ No.of\ CTS + Total\ No.of\ ACK\ frames \tag{12}$$

5.6. Network Throughput

This is the ratio of the quantity of data received from the source to the period the destination node gets the last frame. This is expressed in bits per second or bytes per second. Every protocol aims at high network throughput. One factor that is considered in this work is that during TVLAN defence operations more temporary broadcast domains are created with each having lower throughputs. Also, a higher mobility leads to frequent topology changes which in turn affect datagrams being sent to different destinations.

5.7. Packet Delivery Ratio

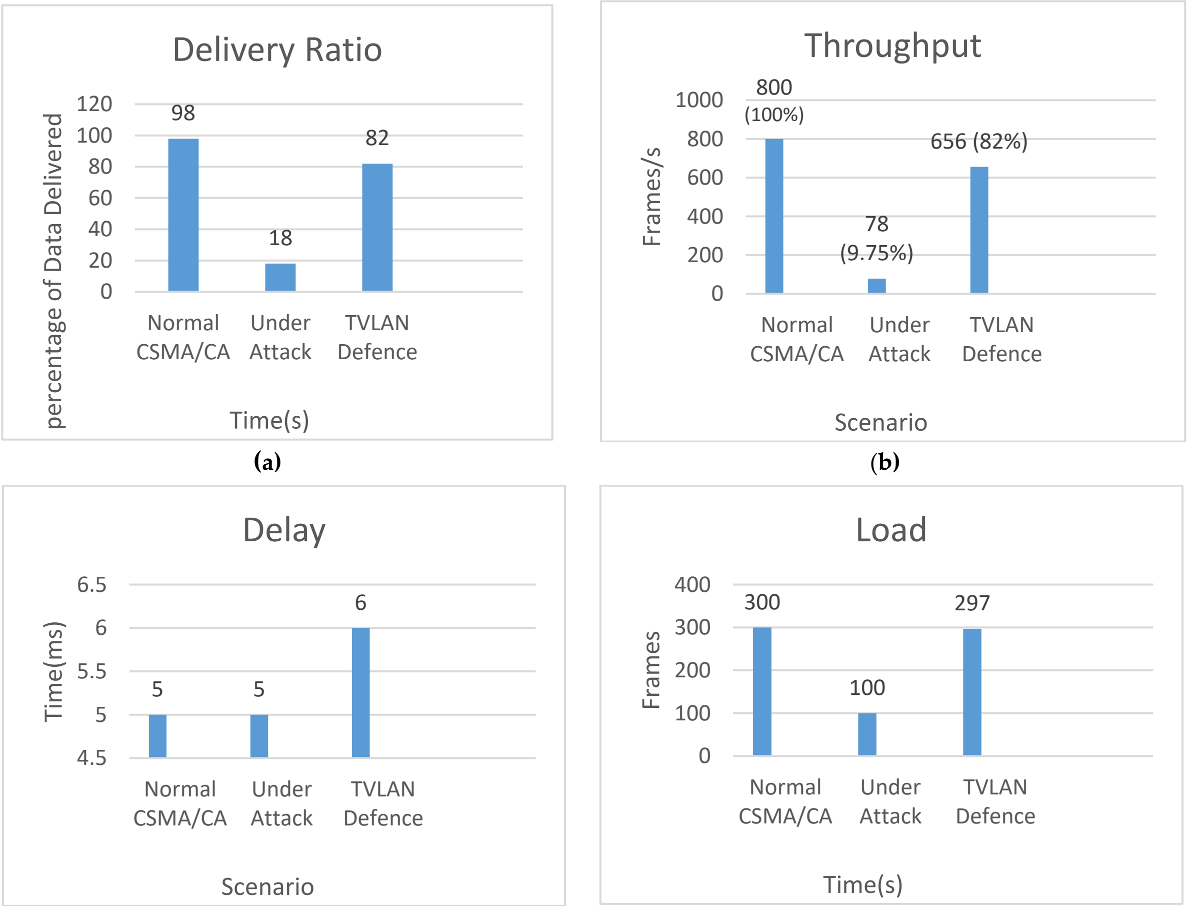
It is the ratio of the data received by the destination node to the data sent by the source node. It effectively measures the loss rate and represents the maximum throughput a protocol can achieve. Every efficient protocol promises a high packet delivery ratio. Here also, mobility must be factored into it.

5.8. End-to-End Delay

It is defined as the average time it takes a packet from the time of generation from the source node till it gets to the destination node. The time taken includes time spent on buffer queue, end-to-end transmission time, and other delays introduced by routing activities such as congestion. Different applications have different levels of tolerance for delays. While an FTP application can tolerate delay up to a certain threshold, voice and video applications require low delays to avoid jitters. End-to-end delay therefore measures the effective reliability of a protocol. A strong factor here is the mobility of the nodes. A higher mobility rate leads to an increase in delay.

6. Results and Discussion

The simulation results for input parameters in Table 2 are discussed in detail in this section. The performance of the proposed TVLAN defence model was evaluated using the four metrics stated above when deployed against a virtual jamming attack. As shown in Figures 5a below, at the point of attack, frame data delivery was reduced to 18% of the normal value. This implies some degree of denial of service to the multi-access channel for nodes intending to send frames. The 18% is the amount of data delivery that the system can offer when under attack. Though very low, the system is not brought under termination of service. This shows the survivability of the system in that it can continue to deliver data though at a reduced rate when under attack. When TVLAN defence was deployed, channel access was restored to 83% of its initial within the experimental time of 10ms thus neutralizing the virtual jamming attack. The system throughput shown in Figure 5b, implies that the system reduced to 9.75% of the original figure. It shows that the system was still functioning when under attack. Though the rate at which service is provided is low, the service was not totally locked down under attack. This showcases the survivability of the system. TVLAN model was able to restore the channel throughput to 82% of its value within the experimental time of 10ms.



(a) **(b)**

(c) **(d)**

Figure 5. Simulation Results displaying Channel Performance: a) Delivery Ratio Performance Result; b) Throughput Performance Result; c) Channel Delay Result and d) Channel Delay Result

Channel delay performance result in Figure 5c showed that the delay when TVLAN was deployed was 1ms higher due to the time it takes for resources reallocation or network partition to smaller broadcast domains and the aggregation process after the attack has been nullified. In Figure 5d, the load is surprisingly much lower when under attack than during normal or defence operations. This is because the jamming attack directly suspends all the control frames. That is, RTS, CTS, and ACK frames that are part of the normal channel load are not functioning. TVLAN restores the native load to almost 100% of its value almost immediately.

7. Conclusion

A torpor-based security model is developed for MANET in this study. The study explored the topology and dynamism of the network to selectively isolate a malicious node from the network. The VLAN technology was used to design a model that easily isolated a jamming node among the participating nodes. The security model was developed to enhance the survivability mechanism for mission-critical systems with CSMA/CA that are susceptible to Jamming attacks and other forms of attacks. The experimental results showed that the model enhanced the performance and survivability of the CSMA/CA when under attack and enabled the network to continue to deliver on its stated mission without degradation. In the face of an attack, the broadcast domain is reduced through fragmentation of the network into two or more VLANs. The torpor-VLAN or TVLAN technique ensures that at the point of fragmentation, the current sending and receiving nodes are partitioned to the same VLAN to prevent data frame loss. The study presents a simple to implement model and at the same an efficient model to combat CSMA/CA threats at TCP/IP layer 1. Further work will be done on how to improve the performance metrics when under attacks and also to use new metrics. After this, we shall be working on full implementation or developing a prototype to be tested with real-life data.

Acknowledgment

The authors acknowledge financial supports from TETFUND and ACE OAK-PARK as well as logistic support from Obafemi Awolowo University for conducting this work research.

References

[1] Deepak Arya, Pramod Mehra, Parag Jain and Abhay Bhatia, "A Study on MANET: Along with Recent Trends, Applications, Types, Protocols, Goals, Challenges", in *Proceedings of the 2023 1st International Conference on Intelligent Computing and Research Trends (ICRT)*, 3-4 February 2023, Roorkee, India, Electronic ISBN: 979-8-3503-3677-1, Print on Demand (PoD) ISBN: 979-8-3503-3678-8, pp. 1-5, Published by IEEE, DOI: 10.1109/ICRT57042.2023.10146716, Available: https://ieeexplore.ieee.org/document/10146716.

[2] Si Liu, Peter Csaba Ölveczky and José Meseguer, "Modeling and analyzing mobile ad hoc networks in Real-Time Maude", *Journal of Logical and Algebraic Methods in Programming*, ISSN 2352-2208, January 2016, Vol. 85, No. 1, Part 1, pp 34-66, Published by Elsevier, DOI: 10.1016/j.jlamp.2015.05.002, Available: https://www.sciencedirect.com/science/article/pii/S2352220815000498.

[3] Luigi Fratta, Mario Gerla and Keun-Woo Lim, "Emerging trends and applications in ad hoc networks", *Annales des Telecommunications/Annals of Telecommunications*, ISSN: 2079-9292, October 2018, Vol. 73, No. 9–10, pp. 547–548, Published by Springer-Verlag, DOI: 10.1007/s12243-018-0662-3, Available: https://link.springer.com/article/10.1007/s12243-018-0662-3.

[4] Sunil Kumar and Kamlesh Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges", *Security and Communication Networks*, 5 May 2016, Vol. 9, No. 14, pp. 2484–2556, Published by John Wiley & Sons Ltd., DOI: 10.1002/sec.1484, Available: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1484.

[5] Norman Islam and Zubair A. Shaikh, "A study of research trends and issues in wireless ad hoc networks", in Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications, Hershey, USA: IGI Global, 2015, ISBN-13: 9781466687516, ISBN-10: 1466687517, EISBN-13: 978146668752, Vol. 4, No. 4, Ch. 81, pp. 1819–1859, DOI: 10.4018/978-1-4666-8751-6.ch081, Available: https://www.igi-global.com/chapter/a-study-of-research-trends-and-issues-in-wireless-ad-hoc-networks/138359.

[6] Diego Santoro, Gines Escudero-Andreu, Konstantios Kyriakopoulos, Franciso J. Aparicio-Navarro, David J. Parish *et al.*, "A hybrid intrusion detection system for virtual jamming attacks on wireless networks", *Measurement*, ISSN: 0263-2241, October 2017, Vol. 109, pp. 79–87, Published by Elsevier, DOI: 10.1016/j.measurement.2017.05.034, Available: https://www.sciencedirect.com/science/article/abs/pii/S0263224117303123.

[7] Hadeel S. Obaid, "Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET", *Journal of Physics: Conference Series*, ISSN**:** 1742-6596, May 2020, Vol. 1530, No. 012009, pp. 1-15, Published by IOP Publishing Ltd, DOI: 10.1088/1742-6596/1530/1/012009, Available: https://iopscience.iop.org/article/10.1088/1742-6596/1530/1/012009.

[8] Boris Bellalta, "IEEE 802.11ax: High-efficiency WLANS", *IEEE Wireless Communications*, Print ISSN: 1536-1284, Electronic ISSN: 1558-0687, February 2016, Vol. 23, No. 1, pp. 38–46, Published by IEEE, DOI: 10.1109/MWC.2016.7422404, Available: https://ieeexplore.ieee.org/document/7422404/1000.

[9] Dimitrios Kosmanos, Apostolos Pappas, Leandros Maglaras, Sotiris Moschoyiannis, Francisco J. Aparicio-Navarro *et al.*, "A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles", *Array*, ISSN 2590-0056, March 2020, Vol. 5, Published by Elsevier, DOI: 10.1016/j.array.2019.100013, Available: https://www.sciencedirect.com/science/article/pii/S259000561930013X.

[10] Farouq Aliyu, Tarek Sheltami and Elhadi M. Shakshuki, "A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing", *Procedia Computing Science*, Online ISSN: 1877-0509, 2018, Vol. 141, pp. 24–31, Published by Elsevier B.V., DOI: 10.1016/j.procs.2018.10.125, Available: https://www.sciencedirect.com/science/article/pii/S1877050918317733.

[11] Ziqian (Cecilia) Dong, Randolph Espejo, Yu Wan and Wenjie Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks", *Journal of Computing and Information Technology*, Print ISSN 1330-1136, Online ISSN 1846-3908, 2015, Vol. 23, No. 4, pp. 283–293, Published by University of Zagreb Faculty of Electrical Engineering and Computing, DOI: 10.2498/cit.1002530, Available: http://cit.fer.hr/index.php/CIT/article/view/2530.

[12] Alejandro Cortés-Leal, Carolina Del-Valle-Soto, Cesar Cardenas, Leonardo J. Valdivia and Jose Alberto A. Del Puerto-Flores, "Performance Metric Analysis for a Jamming Detection Mechanism under Collaborative and Cooperative Schemes in Industrial Wireless Sensor Networks", *Sensors*, ISSN: 1424-8220**,** December 2021, Vol. 22, No. 1, p. 178, Published by MDPI, DOI: 10.3390/s22010178, Available: https://www.mdpi.com/1424-8220/22/1/178.

[13] Huong Nguyen-Minh, Tung Tran Hoang and Giang Pham Thanh, "Machine Learning-Based Jamming Detection for Safety Applications in Vehicular Networks: Individual Detection?", *Security and Communication Networks*, Print ISSN: 1939-0114, Online ISSN: 1939-0122, 12 October 2023, Vol. 2023, Article ID 8080669, pp. 1–12, Published by Hindawi, DOI: 10.1155/2023/8080669, Available: https://www.hindawi.com/journals/scn/2023/8080669/.

[14] Ruichi Zhu, Tao Li and Aiqun Hu, "Efficient jamming attacks in Wi-Fi networks based on legacy short training field", *Journal of Physics: Conference Series*, ISSN: 1742-6596, October 2022, Vol. 2352, No. 012006, Published by IOP Publishing Ltd, DOI: 10.1088/1742-6596/2352/1/012006, Available: https://iopscience.iop.org/article/10.1088/1742-6596/2352/1/012006.

[15] Sun-Jin Lee, Yu-Rim Lee, So-Eun Jeon and Il-Gu Lee, "Machine learning-based jamming attack classification and effective defence technique", *Computer and Security*, ISSN: 0167-4048, May 2023, Vol. 128, Article ID: 103169, Corpus ID: 257323182, Published by Elsevier B.V., DOI: 10.1016/j.cose.2023.103169, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404823000792?.

[16] S. V. Manikanthan and T. Padmapriya, "Detection of jamming and interference attacks in wireless communication network using deep learning technique", in *Proceedings of the First International Conference on Computing, Communication and Control System (I3CAC 2021)*, 7-8 June 2021, Chennai, India, Published by EAI, DOI: 10.4108/eai.7-6-2021.2308599, Available: https://eudl.eu/doi/10.4108/eai.7-6-2021.2308599.

[17] Anh Tuan Giang, Hoang Tung Tran, Huu Ton Le, Nhat Quang Doan and Minh Huong Nguyen, "Jamming Attack in Vehicular Networks: Adaptively Probabilistic Channel Surfing Scheme", *Wireless Communications in Mobile Computing*, Print ISSN: 1530-8669, E-ISSN: 1530-8677, 11 July 2022, Vol. 2022, Article ID: 3884761, Published by Hindawi, DOI: 10.1155/2022/3884761, Available: https://www.hindawi.com/journals/wcmc/2022/3884761/.

[18] Emilie Bout and Valeria Loscrí, "An Adaptable Module for Designing Jamming Attacks in WiFi Networks for ns-3", in *Proceedings of the International Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 24-28 October 2022, Montreal Quebec, Canada, ISBN**:** 978-1-4503-9482-6, pp. 121–124, Published by ACM, DOI: 10.1145/3551659.3559059, Available: https://dl.acm.org/doi/10.1145/3551659.3559059.

[19] Bader A. Aldawsari and Jafar Haadi. Jafarian, "A Jamming-Resilient and Scalable Broadcasting Algorithm for Multiple Access Channel Networks", *Applied Sciences*, ISSN: 2076-3417**,** January 2021, Vol. 11, No. 3, p. 1156, Published by MDPI**,** DOI: 10.3390/app11031156, Available: https://www.mdpi.com/2076-3417/11/3/1156.

[20] Zidong Ming, Xin. Liu, Xiaofei Yang and Mei. Wang, "An Improved CSMA/CA Protocol Anti-Jamming Method Based on Reinforcement Learning", *Electronics (Basel)*, ISSN: 2079-9292**,** August 2023, Vol. 12, No. 17, p. 3547, Published by MDPI**,** DOI: 10.3390/electronics12173547, Available: https://www.mdpi.com/2079-9292/12/17/3547.

[21] Luca Arcangeloni, EnricoTesti and Andrea. Giorgetti, "Detection of Jamming Attacks via Source Separation and Causal Inference", *IEEE Transactions on Communications*, Print ISSN: 0090-6778, Electronic ISSN: 1558-0857, August 2023, Vol. 71, No. 8, pp. 4793–4806, Published by IEEE, DOI: 10.1109/TCOMM.2023.3281467, Available: https://ieeexplore.ieee.org/document/10138559.

[22] Ashraf Al Sharah, Hamza Abu Owida, Talal A. Edwan and Feras Alnaimat, "A Cooperative Smart Jamming Attack in Internet of Things Networks", *Journal of information and communication convergence engineering*, Electronic ISSN: 2234-8883, Print ISSN: 2234-8255, 21 December 2022, Vol. 20, No. 4, pp. 250–258, Published by Korea Institute of Information and Communication Engineering, DOI: 10.56977/jicce.2022.20.4.250, Available: https://www.jicce.org/journal/view.html?uid=1194&vmd=Full.

[23] Ahmet Cetinkaya, Hideaki Ishii and Tomohisa Hayakawa, "Effects of Jamming Attacks on Wireless Networked Control Systems Under Disturbance", *IEEE Transactions on Automation and Control*, Print ISSN: 0018-9286, Electronic ISSN: 1558-2523, February 2023, Vol. 68, No. 2, pp. 1223–1230, Published by IEEE, DOI: 10.1109/TAC.2022.3153275, Available: https://ieeexplore.ieee.org/document/9721128.

[24] Markus H. Schmidt, "The energy allocation function of sleep: A unifying theory of sleep, torpor, and continuous wakefulness", *Neuroscience and Biobehaviour Reviews*, Print ISSN: 0149-7634, Online ISSN: 1873-7528, November 2014, Vol. 47, pp. 122–153, Published by Elsevier B.V., DOI: 10.1016/j.neubiorev.2014.08.001, Available: https://www.sciencedirect.com/science/article/pii/S0149763414001997.