SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I7P101

Volume 10 Issue 7, 1-12, July 2023
© 2023 Seventh Sense Research Group®

Original Article

Detection System using Random X-Layer Mobility with QCH Algorithm in Wireless Ad-hoc Networks

S. Sandosh[1], P. Saravanan[2], D. Shofia Priyadharshini[3], G. Anitha[4]

[1]School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Chennai, India.
[2]Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai, India.
[3]Department of Electronics and Communication Engineering, VelTech Hightech Dr Rangarajan Dr Sakunthala Engineering College, Chennai, India.
[4]Department of Electronics and Communication Engineering, RMD Engineering College, Chennai, India.

[1]Corresponding Author : sandosh.s@vit.ac.in

Received: 16 April 2023 Revised: 18 June 2023 Accepted: 09 July 2023 Published: 31 July 2023

***Abstract** - Intrusion Detection Systems (IDS) are critical in identifying malicious activities that degrade network performance. An ad hoc system is a self-organizing, transient network with no infrastructure. Because of its open medium, constantly shifting topologies, co - operative protocols, loss of centralised monitoring and administration point, and absence of a distinct line of protection, wireless ad-hoc networks are especially susceptible. Many intrusion detection methods built for fixed wired networks are no longer relevant in this new context. Then, we present the novel IDS and response techniques we are working on for wireless ad hoc networks (WANet). This research presents two IDS techniques. Using the permissive mode in line with the location of the nodes throughout the simulation is the first technique. Within the AODV Routing protocol context, this method is known as the quasi-cluster head (QCH) algorithm. The given simulation area is segmented into four quadrants, each having a circular inside the centre. Each node will be able to collect data via neighbours within the radio transmission range. X-layer IDS with Random X-Layer Mobility is the second technique. We are developing tools to identify ad-hoc basis flooding, routing disruption, and dropping attacks against WANet. On simulation model networks, the effectiveness of evolved programmes is evaluated.*

***Keywords** - Intrusion detection systems, QCH algorithm, AODV, X-layer IDS, WANet, Random X-layer mobility.*

1. Introduction

A mobile ad hoc network is a kind of network that is both smaller and transient. This network operates on a fundamentally different concept and has a fundamentally different structure from wired networks. Intermediary nodes transfer data from the source node to the destination node. A strategy for finding neighbours in static settings that considers energy considerations and uses randomized handshakes [1].

Regarding energy consumption, the proposal's performance is superior to that of the reference protocol in one- and multi-hop situations. There has been much dispute over apparent inconsistency in the network's ad-hoc intrusion detection architecture, with different intrusion detection algorithms operating in cluster- or host-based settings [2]. Host- or cluster-based methods have advantages and disadvantages, including the network's capacity to maintain security even if a cluster head is replaced late.

The cluster technique carries significant weight since it can quickly detect black hole attacks on various networks, including wireless ad hoc networks (WANET), MANET and much more. [3]. After the development of wireless ad hoc networks that do not possess a communications backbone, the first stage of the utmost importance is called "neighbour discovery." Analytical models of randomized neighbour-finding techniques for static one-hop settings are presented by us in this study [4]—an undeniable benefit regarding the amount of energy used and the number of packets sent. Dynamic topologies and high node mobility are two distinguishing features of wireless ad hoc networks. Attacks on wireless ad hoc networks may considerably impact performance parameters such as the percentage of packets delivered from the source to the destination node, overhead, and throughput [5].

Mobile ad hoc networks are wireless networks that may self-organize and quickly deploy. These networks are helpful for external events, communications in areas without radio infrastructure, natural catastrophes, and military operations. Because of the fluidity and changeability of network topologies, security may be the weakest link in the network. This leaves it susceptible to various threats, including eavesdropping, routing changes, and application modifications [6]. There are more vulnerabilities in MANET's security than there are in its quality of service. There has recently been a significant increase in the development and deployment of Ad-hoc to manage massive traffic volumes efficiently and securely. Implementing security measures to guard against the abovementioned dangers is critical [7]. Such networking, however, is vulnerable to various cyber-attacks on the network's data security, confidentiality, verification, and reliability.

Mobile computing is the more robust network communication and connection usage, thanks to recent breakthroughs in wireless networks or MANETs. The creation of successful networks is fraught with a myriad of challenges [8]. Networks must be able to transport data from one system to another while maintaining acceptable accuracy. A framework is required for most applications to verify that the recovered data is compatible with the data sent [9]. If the frame sent between the two nodes in the data-link layer is distorted in any way, it has to be rectified before it may be driven to other nodes. The showing of excellent nodes is significantly tainted by deviant nodes that refuse to conform to the norm. As a result, a method for detecting intrusions must be included in the MANET [10].

The nodes of WANET intercommunicate through wireless connections directly or by relying totally on neighbouring nodes as routers. The most common causes of packet loss in WANET [11] are intentional packet-dropping attacks and problems at the link level. An offline process is used to define monitored in a dynamic manner when the network is in operation [12]. The term "black hole attack" describes an attack carried out on a MANET by a hostile node that fraudulently alters the sequence number & hop count of the routing message to forcefully acquire the route from a source to a destination [13]. The term "selected black hole" refers to a node that can either carry out an attack similar to a black hole or perform its regular functions.

A mobile ad-hoc network is a dynamically wireless network that transports data between neighbour nodes using a temporary configuration. Mobile ad-hoc networks are also known as mesh networks. It is vulnerable to assaults and incursions [14] because of the dynamic nature of the system. Attacks that interrupt routing are the primary concern in this network, which is plagued by hostile behaviour from intermediate nodes. Effective first-line defence systems often consist of data protection mechanisms based on encryption. It is not compatible with the environment of the mobile ad-hoc network. By honestly and efficiently selecting the node within the cluster with the lowest overall cost of operation, often referred to as the leader-IDS, one can bring the resource consumption of all the nodes into a more even distribution and, as a result, extend the overall lifespan of the cluster.

The following paper deals with section 2 gives related works based on IDS; section 3 provides the proposed methodology of our research; section 4 states the experimental setup with its performance analysis; and section 5 follows with a conclusion.

2. Related Works

Wireless-specific traffic characteristics with a significant information gain are often located in the data link levels instead of the application layers. The experimental findings indicate that the average detection efficiency for a blackhole assault is 94.37%, while the detection accuracy for a wormhole attack is 99%. The performance of the suggested approach [16] is superior to current intrusion detection methods. Implementing an intrusion detection system in a wireless environment is not as easy as in a wired network owing to the complexity of the architectural setup [17]. Consequently, developing an IDS that focuses exclusively on wireless networks is of the utmost importance.

The proposal's performance is superior to the reference protocol [18] in environments with one hop, environments with multiple hops that are discovered, and the number of discoveries that occur for each packet sent when the duty cycle is high. Host-based networks can maintain their security even if there is a lag in replacing a cluster head. However, several academics have proposed [19, 20] various approaches for improved anomaly detection in the network.

The study methodology component articulated the general procedure of concluding the clustering strategy's efficiency clearly and concisely [21, 22]. After that, the discussion portion supplied a precise technique by which black holes may be readily found. This was accomplished by following the previous steps. Analytical models of randomized neighbour-finding techniques for static one-hop settings were given in this study [23]. An undeniable benefit is the energy used and the number of packets sent.

Investigations are being conducted into the dependency of features on the nature of network traffic and the dependencies of performance measures on the velocity of mobile nodes within the network. The efficiency of an intrusion detection system based on simulated data was shown by the experimental experiments carried out and reported in [24, 25]. Monitoring for undesired access is essential to preventive and further security measures against unauthorized entry [26]. The capacity of a mobile node to forward packets, dependent on the system's life as a whole, may be hampered if the node's power supply were unavailable. The IDS assigns a value of 0 or 1 to each branch of a sequence according to the reconstructed error threshold for that branch [27]. The security vulnerabilities that have been detected in the engine of the intrusion detection system may be threatened by the assaults that occur in the network; however, the intrusion prevention engine in the network can stop these attacks from happening [28].

A wireless ad-hoc network is a collection of hubs that uses a wireless channel to communicate with one another and coordinate their actions to establish information exchange between any pair of hubs [29]. This type of network does not have a centralized structure. When it comes to using MANETs, one of the most significant challenges is the problem of data security.

[30] Various factors, including link errors and the incidence of malicious assaults, may cause packet loss. The authentication service is provided inside this protocol to achieve specified performance. In addition, the first stage is responsible for tuning and calibrating the second stage. In the second step of the process, a cross-correlative element is used to detect several threats all at once [31].

A node that can execute either a black hole attack or standard node functions might be described as having selective black hole capabilities [32]. In order to carry out the so-called ABM, the IDS nodes must be configured to operate in sniff mode. In this review study [33], the authors evaluated works connected to implementing the IDS in the VANET region. They also offered a theoretical notion about building the IDS system to protect the network and prevent any harm caused by an attack. The findings obtained [34] show that the proposed system can achieve high detection accuracy, a low false alarm rate, and low energy consumption, positioning it as a suitable IDS option for wireless sensor networks.

The information categorization system is learned using the suggested technique [35], and the experimental results demonstrate that the proposed method works better than other existing methods. By accurately and expeditiously selecting the node in a cluster that has the lowest overall cost of operation, also referred to as the leader-IDS, it is possible to achieve a better equilibrium in the consumption of resources across all of the nodes and, as a result, to extend the total lifetime of the cluster.

Using simulations, it was determined that both algorithms provide satisfactory performance even when message losses occur due to an unstable channel [37, 38]. The primary purpose of this research is to investigate the numerous varieties of IDS already in use in WANets for intrusion detection and to understand the difficulties and advantages presented by each approach. We sincerely hope this body of work will one day be a helpful resource for researchers actively engaged in this study area.

3. Proposed Methodology

This section presents a suggested technique for dividing the field of operations across small squares, with an imaginary circle in the middle of each square. When a network joins the circular, it joins permissive status; the cluster then works as a Quasi cluster head (QCH), receiving data from its neighbouring access points within every quadrant of both the area and utilising this data to develop an anomaly index (AI) within every quadrant. The AI that has been calculated is delivered to the Controller, which also functions as a control and command unit as well as quantifies connectivity AI.

We suggest a technique in which the area of action is split into smaller squares, with an imaginary circle in the middle of each square. When a node enters the circle, it enters permissive mode and acts as QCH. Figure 1 depicts a view of the network deployment created by NS3's Network Simulator tool.

Every circular has to have a circumference of 100m, and its midpoint is located at the curve in each of the four QCH sectors. The data from QCH will be utilised to create an AI for each quartile. The computational AI will be communicated to the Controller, which serves as a controlling and command unit and provides network-level AI. The QCH evolves with time, whereas the Controller is a permanent position.

```
Algorithm 1: QCH algorithm
    Positioning of nodes - equal allocation
    Create k permissive regions of radial distance r.
    Set node 12 to be a respond.
    Began nodes - connectivity in consonance with the
    model of mobility
    Repeat
    If the node is located in the promiscuity area, then...
    Connect with neighbors
    AI Computation Detection
    AI – Controller detection of Transmit
    end if
    maintain the current state
    End until simulation gets completed
```

Algorithm 1 describes the simulation method. The nodes in the grid are initially distributed uniformly throughout the grid. Then, with a radius of r, we create k circular promiscuity zones. The unusual networking profile is built by identifying node 12 as a response & executing it for 2000 s at eight distinct times. Furthermore, all mobile nodes employ the Random X-Layer mobility (RXM) model.

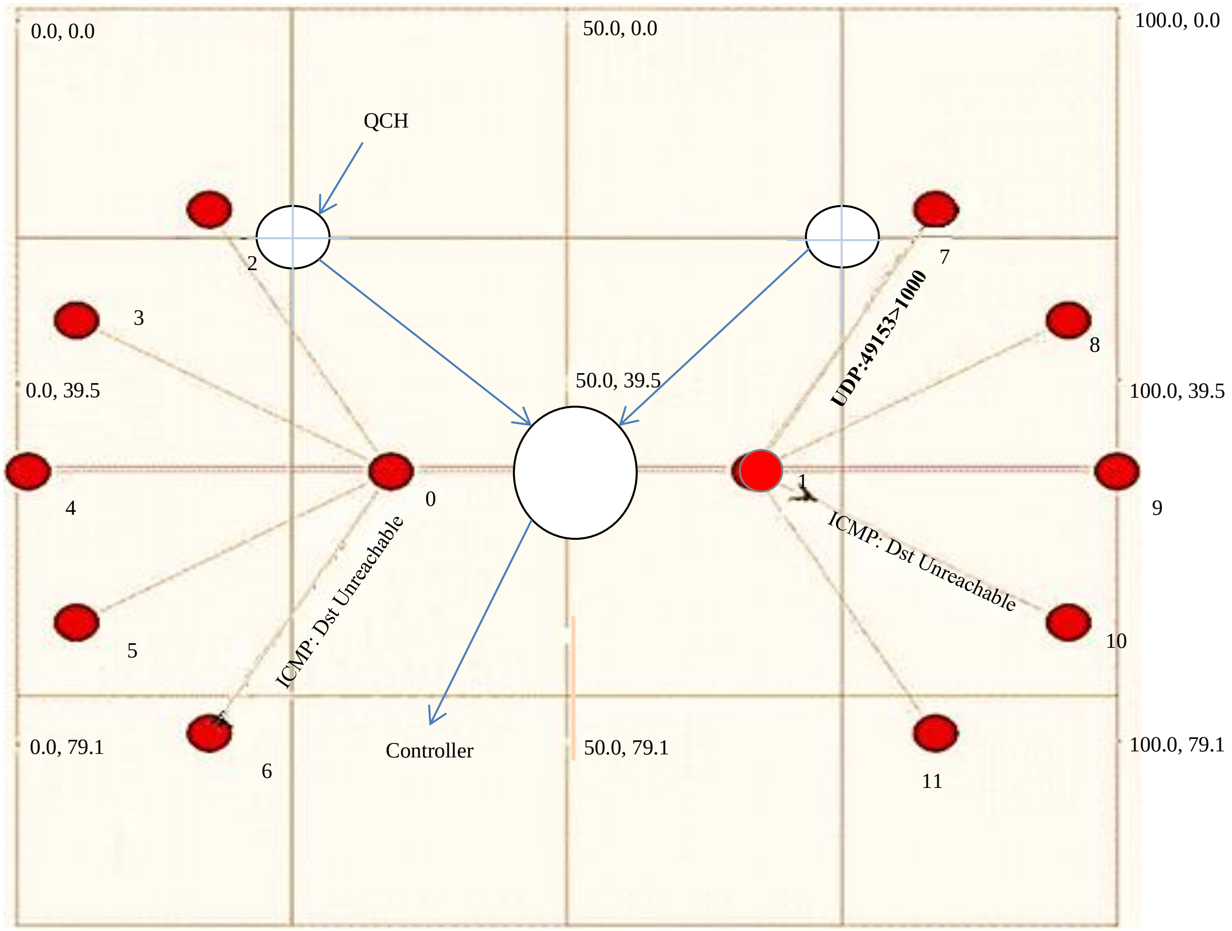

Fig. 1 A QCH-Based IDS method

3.1. Ad Hoc On-Demand Vector (AODV)

Many routing protocols have been suggested to meet the various demands of WANets. Unfortunately, most of these routing technologies do not consider security. AODV routing protocol is one of the most widely used. Within the scope of this research, the AODV routing protocol is implemented. AODV is a dynamic routing technique that finds routes only when needed. It offers quick flexibility to changing connection conditions, little processing and storage latency, and limited bandwidth use. AODV is reportedly capable of managing low, intermediate, and slightly higher wireless frequencies and various data traffic loads. However, it does not have any security measures.

AODV communications are classified into three types: 1. Route Request (RREQ), 2. Route Reply (RREP), and 3. Route Error (RERR). When an access point desires to communicate with another communication link but has no new path to this destination, it starts the route-discovery process by sending an RREQ packet to the destination node. Whenever destination nodes receive this message, they transmit an RREP towards the source host if there is a new path to the target node, and they transmit a target RREP.

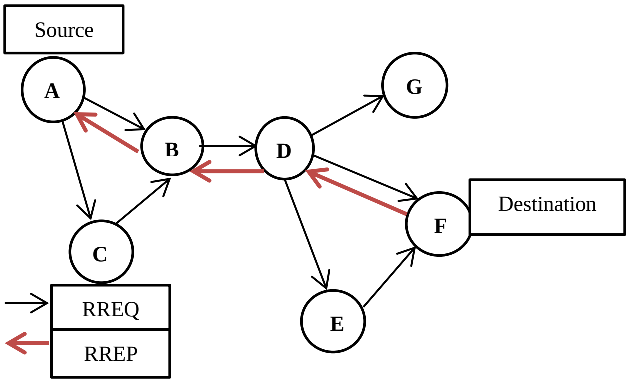

Fig. 2 AODV route discovery

Figure 2 shows a simplified connection between source A and node F. The source (A) begins an RREQ that is disseminated to the neighbours. If an access point can communicate with the destination address, it will return an RREP message to the source.

Whenever the source node gets the RREP, it begins transferring data along a route identified during much of the discovery of the route. It is critical to notice that the RREQ has a characteristic known as the sequence number, which specifies the route's validity, making it more appealing to transmit data over it.

If a link disconnect takes place between the nodes that are spatially closest to the intermediate nodes, the node that is closest to the target node will send a RERR message to the node that is further away from the source in order to notify the source node that the receiver is no longer reachable and must re-establish a connection route discovery, as shown in figure 3.

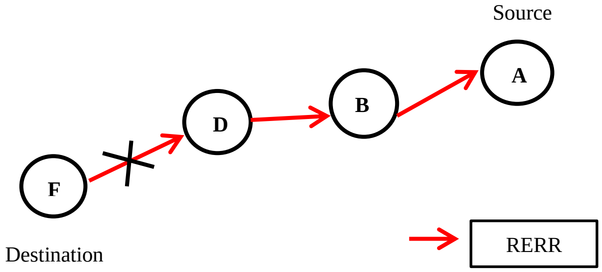

Fig. 3 Link maintenance in AODV

3.2. Random X-Layer Mobility

Because of its simplicity and availability, the Random X-Layer Mobility (RXM) Model is a "benchmark" mobility model for evaluating WANet routing methods. The RXM paradigm is far and away the most popular methodology used in modelling next-generation wireless networks, and it is the flexibility that is defaulted in many different system simulators. During the simulations, each node randomly chooses a destination location from the available options. It then moves with constant velocity towards this destination, using uniform random variables from [0, Vmax], where Vmax refers to the highest velocity each mobile node may maintain. Each node in the simulation region independently chooses its velocity & direction of travel. When the node arrives at its goal, it chooses another route and proceeds. As illustrated in Fig 4, a pause time (Tpause) may be incorporated into the simulation to cause the node to halt for a while.

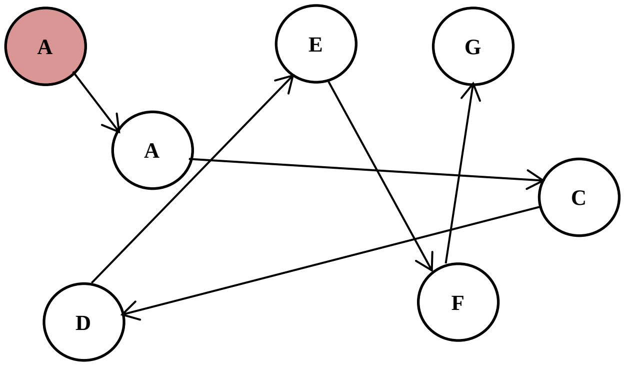

Fig. 4 An example of node movement is shown

$$f(l) = \frac{4l}{x^2y^2} f(Len) \qquad (1)$$

$$f(Len) = \left\{ \begin{array}{l} \frac{\pi}{2}ab - al - bl + \frac{1}{2}l^2 \\ \quad for\ 0 \le l \le b \\ absin^{-1}\frac{b}{l} + \sqrt[a]{l^2 - b^2} - \frac{1}{2}b^2 - al \\ \quad for\ b < l < a \\ absin^{-1} + \sqrt[a]{l^2 - b^2} - \frac{1}{2}b^2 - al \\ \quad for\ a \le l \le \sqrt{a^2 - b^2} \\ -abcos^{-1}\frac{a_1}{l} + \sqrt[b]{l^2 - y^2} - \frac{1}{2}x^2 - \frac{1}{2}l^2 \\ 0 \qquad otherwise \end{array} \right\} \qquad (2)$$

Similarly, the value that is estimated for the length of the transition L is

$$E(Len) = \frac{1}{15}\left[\frac{x^3}{y^2} + \frac{y^3}{x^2} + \sqrt{x^2 + y^2\ (3 - \frac{x^2}{y^2} - \frac{y^2}{x^2}}\right] + \frac{1}{6}\left[\frac{y^2}{x}cosh^{-1}\sqrt{\frac{x^2+y^2}{y}} + \frac{y^2}{a}cosh^{-1}\sqrt{\frac{x^2+y^2}{y}}\right] \qquad (3)$$

And the variation of transition duration L is

$$E\ [Len^2] = \frac{1}{6}\ (x^2 + y^2) \qquad (4)$$

3.3. X-Layer Intrusion Detection Systems (X-Layer IDS)

An intrusion is any collection of activities that undermine a resource's integrity, confidentiality, or reliability. The following elements drive the creation of an IDS: Most current systems include security flaws that make them vulnerable to breaches, and discovering and correcting them is impossible. Prevention tactics alone will not suffice. It is almost hard to create an entirely secure system. Insider assaults may compromise even the most secure systems. New invasions regularly arise, necessitating the development of new defence measures.

Because fresh intrusions cannot be avoided, intrusion detection systems (IDS) are used to identify potential activity and reaction. If we notice the assault as soon as it enters the network, we may launch a reaction to avoid or minimize system damage.

It also aids in improving preventive strategies by giving information on incursion tactics. Our IDS design adheres to the classic layered architecture and employs the notion of communication through a cross-layer entity known as X-Layer IDS. This decision is based on the layered architecture's many advantages, notably flexibility, which contributes to the architecture's lifespan and compliance with the OSI model. An X-layer entity allows for cross-layer individual development that extends to both layers, including the thing itself, without disrupting the overall system. Another benefit is that this entity has unrestricted access to all levels, allowing for more objective judgements. In addition, it permits the straightforward and uncomplicated inclusion of new cross-layer data and algorithms without necessitating modifications to the remainder of the architecture. The suggested X-layer architecture is shown in Figure 5.

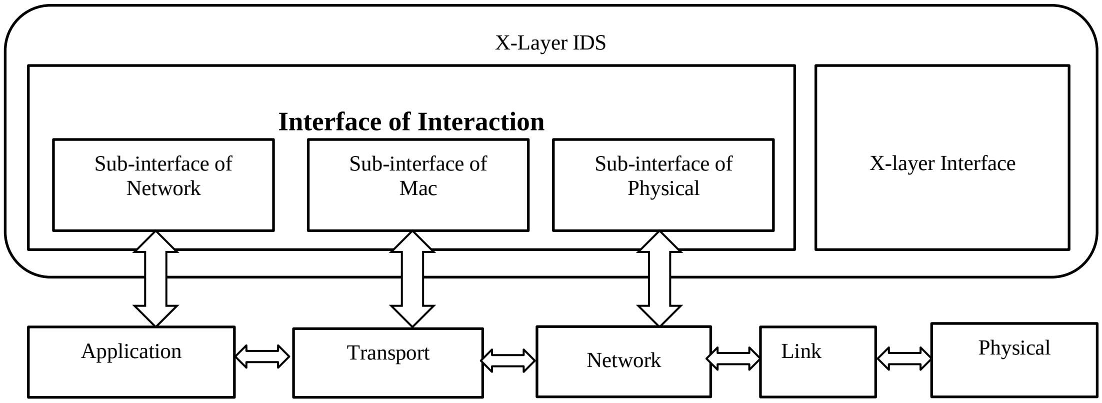

Fig. 5 X-Layer proposed architecture

The X-Layer IDS is the mechanism through which the layers & applications interact. It consists of 2 parts: the Interface of interaction & the X-layer Interface.

The interaction interface promotes communication among the layers and applications on the one hand and the X-Layer system on the other. The interaction interface's primary goal is to manage the sub-interfaces that allow access to the layers. Each sub-interface provides techniques for reading and writing to aid in manipulating protocol parameters. These techniques are used to acquire and update data.

The X-Layer Interface expresses data uniquely, allowing all layer protocols to access it readily. This module's data is the foundation for every X-layer adaptation & optimization. The module is also in charge of keeping data up to date through the X-layer interface of interactions.

The suggested IDS is built on an X-layer architecture that uses the interaction and cooperation of three OSI model layers: network, Mac, and physical. Our intrusion detection system's core concept is to identify intruders when they try to connect with network nodes.

Our detection algorithm analyzes whether the targeted node is one of the neighbours in the routing route after obtaining RTS (Request to Send) packets from the invader's node. Furthermore, the intruder node's validity will be verified by evaluating the receiving packet's RSSI (Received Signal Strength Indicator). Each sensor node may anticipate the source of packets that will be transmitted by leveraging routing information at its MAC layer. As a result, if a node is not included in the routing route and attempts to communicate (receive RTS packets) with the sensor nodes, it is instantly identified as an intruder.

When a node gets a packet, unless specified authentication is employed RSSI, it is impossible to determine whether the packet originated from the stated sender. TinyOS, a recently suggested embedded operating system, can obtain the RSSI value. As demonstrated in Figure 6, the received signal intensity for a wireless medium is proportional to the distance between nodes.

At its physical layer, all nodes are aware of the relative transmit power of the packets their neighbours are sending. As a result, the legitimacy of the intruder node may be determined since the signal intensity of the packets is not equal to the computed RSSI. The detecting ability is, therefore, considerably increased by integrating RSSI value with the neighbourhood routing database.

$P_{Detection}$, the likelihood of detecting an intruder, is determined by the presence of targeted nodes within a cluster and the likelihood of an impacted node being overlooked during detection. We determined that A was the number of nodes targeted in the assault. The intruder node cannot be identified in our X-Layer IDS until the attacked node receives no packets from the intruder node. Therefore, the probability of delayed detection is equivalent to the risk of a collision occurring in data transmission.

$P_{Collision}$ Using the Binomial rule, we can calculate the likelihood of detecting an intruder as follows:

$$P_{Detection} = \binom{A}{1}(1 - P_C){P_C}^{X-1} \quad (5)$$

We can compute the likelihood of detecting X intruder into the network using equation 6:

$$P_{Detection} = \binom{A}{X} (1 - P_C)^A {P_C}^{X-1} \qquad (6)$$

In our idea, all network nodes can identify intruders, and the likelihood of detection increases steadily as the number of assaulted nodes increases, and the level of cooperation decreases. On the other hand, most suggested X-Layer IDS require increasing the no. of monitor nodes to improve detection probability, which is inefficient in terms of energy.

We expect the invader node to assault all nodes within its radio antenna's range. As a result, the maximum number of nodes assaulted by an intruder may be equal to:

$$Average = (N-1)\, pr^2/area \qquad (7)$$

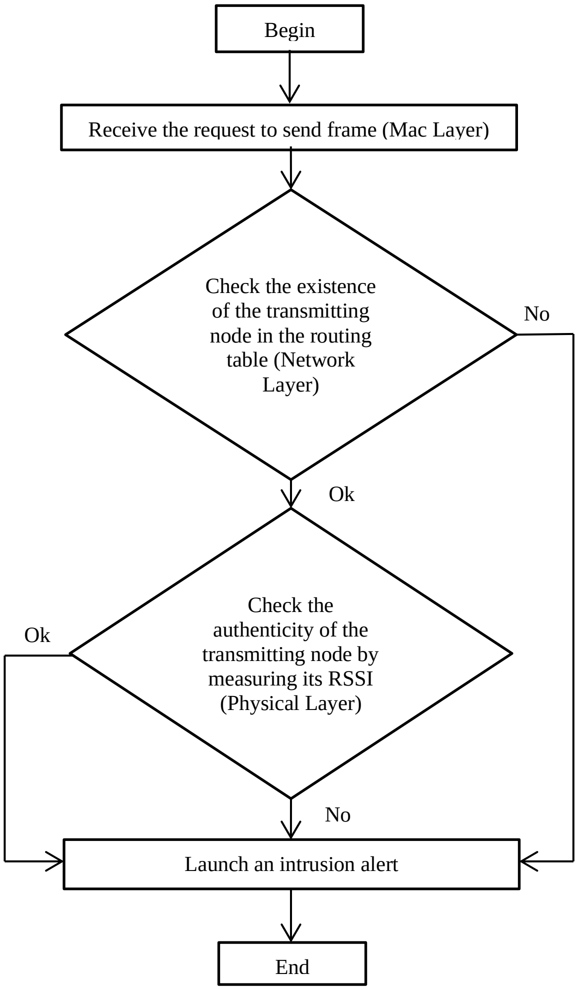
Begin
Receive the request to send frame (Mac Layer)
Check the existence of the transmitting node in the routing table (Network Layer)
No
Ok
Check the authenticity of the transmitting node by measuring its RSSI (Physical Layer)
Ok
No
Launch an intrusion alert
End

Fig. 6 Our suggested IDS's algorithm

Where N indicates the number of nodes in each zone, the area seems to be the range region, and r denotes the intrusion broadcasting radius.

We suggested X-Layer IDS is energy efficient since we reuse data created by the network, Mac, and physical layers. As a result, our technique incurs minimal extra cost and is therefore well suited for resource-limited WANet. We compute the spent energy of our X-Layer IDS on each attacked node to determine the overall energy used by our X-Layer IDS.

$$Energy\ Assumed = E_R + E_I + E_A \qquad (8)$$

E_R denotes the power used when receiving a packet from an intruder, E_I denotes the power consumed while executing the intruder detection algorithm, and E_A denotes the power consumed while sending the alarm message. The amount of energy used by our X-Layer IDS to protect the networks from x attacker (at) nodes is thus equal to:

$$Energy_X - Layer\ IDS = \sum_{a=0}^{X} \sum_{i=0}^{A} Energy\ reduced \qquad (9)$$

In contrast to conventional IDS (which employ fixed monitoring nodes), our X-Layer IDS consumes less energy when the number of intruders and attacked nodes drops. This saves energy and increases network longevity.

3.4. Gauss-Markov Mobility

In this model, node velocity $n(v)$ is coupled in time and is represented by a Gauss-Markov random process. If the stationary Gaussian process $n(v)$ has the autocorrelation function, it is a Gauss-Markov process.

$$R(T) = F[n(v)\, n(v+r)] = \sigma^2 e^{-\beta} + \mu^2 \qquad (10)$$

Where $s^2$the variation of is $v(t)$, ? is the mean, and 0 is the degree of memory. In equation 11, the discrete form of velocity is expressed as V_m, and the memory level is displayed.

$$V_m = aV_{m-1} + (1-\alpha)\vartheta + \sigma\left(\sqrt{1 - a^2}\right) w_{m-1} \qquad (11)$$

V_m is an uncorrelated Gaussian process with zero mean and one unit of variance, which is not dependent on V_m. Equations 12 and 13 show that it comprises two parts: the intensity and the direction.

$$|V_m| = \alpha |V_{m-1}| (1-\alpha)\mu_{|v|} + \sigma_{|v|}\left(\sqrt{1 - a^2}\right) w_{|n-1|} \qquad (12)$$

$$\theta_m = \alpha\theta_{m-1} + (1-\alpha)\mu_{\theta} + \sigma_{\theta}\left(\sqrt{1 - a^2}\right) w_{\theta|m-1|} \qquad (13)$$

The future position of the mobile node may be determined at each time interval depending on its present location, direction of travel, and speed.

$$X_n = X_{n-1} + |v_{n-1}|cos\theta_{n-1} \quad (14)$$

$$Y_n = Y_{n-1} + |v_{n-1}|cos\theta_{n-1} \quad (15)$$

Where (X_n, Y_n) and (X_{n-1}, Y_{n-1}) are the x and y coordinates of the mobility location at the nth and (n-1)st time interval and |V_(n − 1) | and θ_(n − 1) are the values that indicate the direction and speed of the access point when at (n − 1)st interval of time, respectively.

4. Experimental Settings

The network behaviour was simulated using the discrete event networks simulator NS3. Table 1 summarizes the key experiment parameters. When nodes leave promiscuity zones, they are set to normal, and when they enter them, they are set to permissive. When the node enters the permissive mode, it will start sniffing the neighbours within its radio transmission range and computing the incursion threshold. This value is then sent to the control node once processed.

Table 1. Simulation settings

No.of Nodes	100
Mobility Model	Random X-Layer
X_dimension of topography	1000
Y_dimension of topography	1000
Routing protocol	AODV
Data type	UDP
Time of simulation end	150 sec
MAC type	Mac/802_11
Range	250m

A sample time of ten seconds is used in the method just described to gather the scores of a group of features that characterise the activities of the nodes. The training lasted for two thousand and zero seconds, with ten seeds each. In each example, a profile was generated for each trait stated earlier, and the results were averaged over the number of nodes. When the QCH travels into the permissive zone, it picks up the qualities listed below. The following types of features are used by our organisation, as shown in Table 2.

Table 2. An experiment with X-layer characteristics

MAC Type	Transmit and Receive RTS	Transmit and Receive CTS	Transmit and Receive ACK
Network Type	Transmit and Receive RREQ	Transmit and Receive RREP	Transmit and Receive RERR

4.1. Performance

The detection rate is the percentage of network intrusions correctly identified relative to the overall number of network invasions. The percentage of networks or systems identified as intrusions is the false positive rate (FPR). This percentage is calculated as a fraction of the regular communication channels. In intrusion detection, an acceptable low percentage of false alarms is just as crucial as actual alerts. A high FPR will cause a significant amount of additional time and will very certainly undermine confidence in the IDS.

$$Detection_{rate} = \frac{correctly\ detected\ attacks}{total\ attacks} \quad (16)$$

$$False_{positive\ rate} = \frac{normal\ activities\ incorrectly\ detected\ as\ attacks}{total\ normal\ attacks} \quad (17)$$

$$Fitness = Detection_{rate} - False_{positive\ rate} \quad (18)$$

Figures 7, 8, and 9 illustrate that the three most influential factors are mainly based on the variation in message counts among the normal and malicious states, even though no method for feature selection was employed in this experiment. This is although no feature engineering method was used in this experiment.

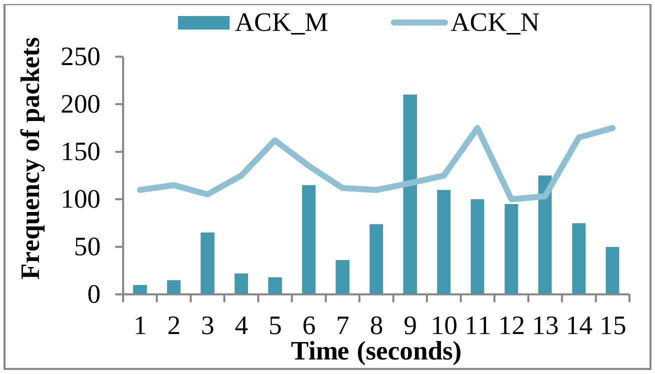

Fig. 7 The amount of ACKs issued in malicious and non-malicious situations

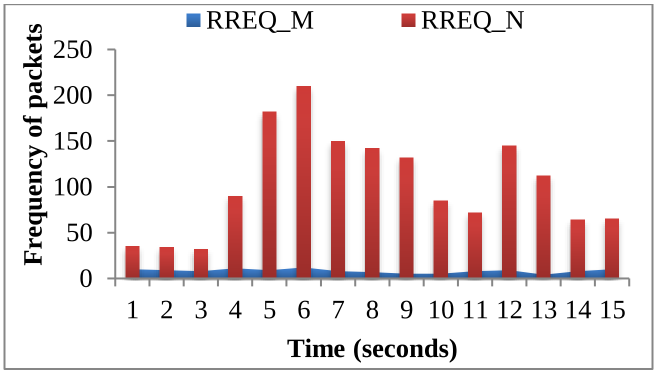

Fig. 8 The amount of RREQs transmitted under both malicious and normal conditions

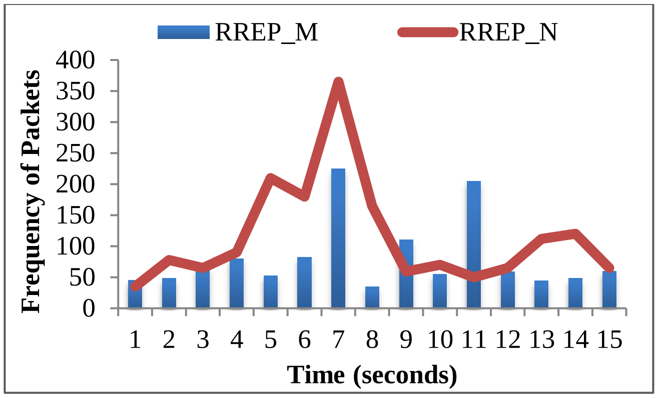

Fig. 9 The amount of RREPs transmitted in both malicious and non-malicious situations

Accuracy for each class is shown in Table 3, and the last row indicates how the weight is distributed across the different network types, malicious and standard.

Table 3. Class-specific accuracy

Weight Distribution Class	True Positive Rate (TPR)	False Positive Rate (FPR)
Normal	0.87	0.02
Weighted Average	0.97	0.02
Malicious	0.89	0.05

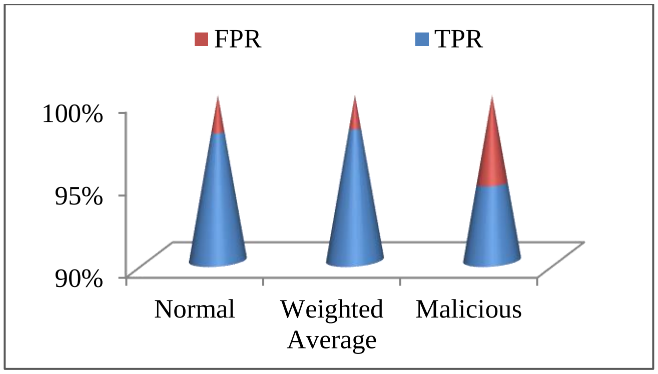

Fig. 10 Accuracy by class

Table 4. Performance of proposed IDS with different attacks

Attacks	Detection Rate (%)	False Positive (%) With Mobility
Ad hoc flooding	99	2.18
Route disruption	99.98	0.91
Dropping attacks	99.99	8.21

According to Table 4 and Figure 11 findings, the FPR produced by detecting an ad-hoc_flooding attack on a current network is higher than the rate produced for a mobile network. This is to be anticipated, given that the programs have matured under medium mobility.

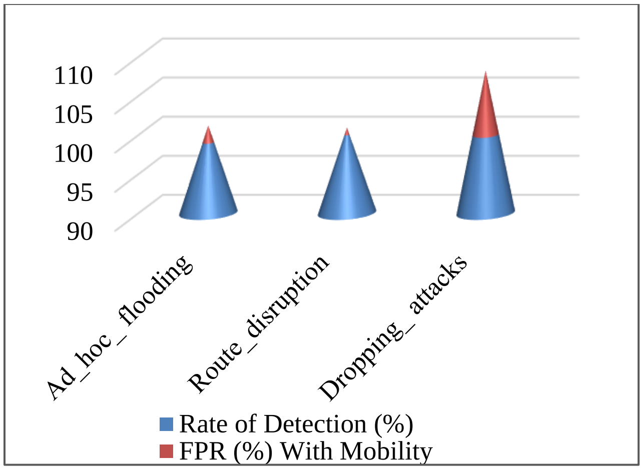

Fig. 11 Proposed IDS with different attacks

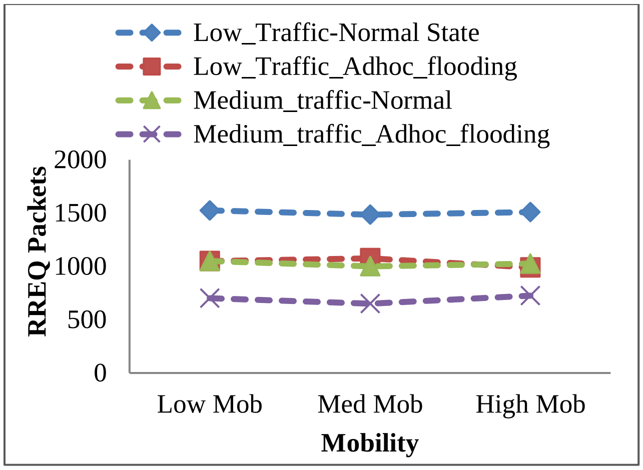

Fig. 12 Request packets to route

Furthermore, several route request messages have been seen in the stable network. It was revealed that the rate of false positives for detecting path disruption attacks is considerably more significant on the network that is now under attack than the network that has not been subjected to any attacks.

The number of route discovery processes on ordinary networks and the number of RREQ on a network that was flooded by ad hoc traffic is shown in Figure 12. There is just a minute variation in the number of RREQ packets sent by networks with varying degrees of mobility. The network with a low to moderate movement may broadcast a substantial proportion of RREQ packets to construct and manage its active routes. This is because of the topology of the network, as well as the mobility and traffic patterns.

In conclusion, accessibility is not the only key factor that plays a role in determining the number of RREQ packets that are sent over the network. Consequently, these features also impact the effectiveness of the programmes that have emerged.

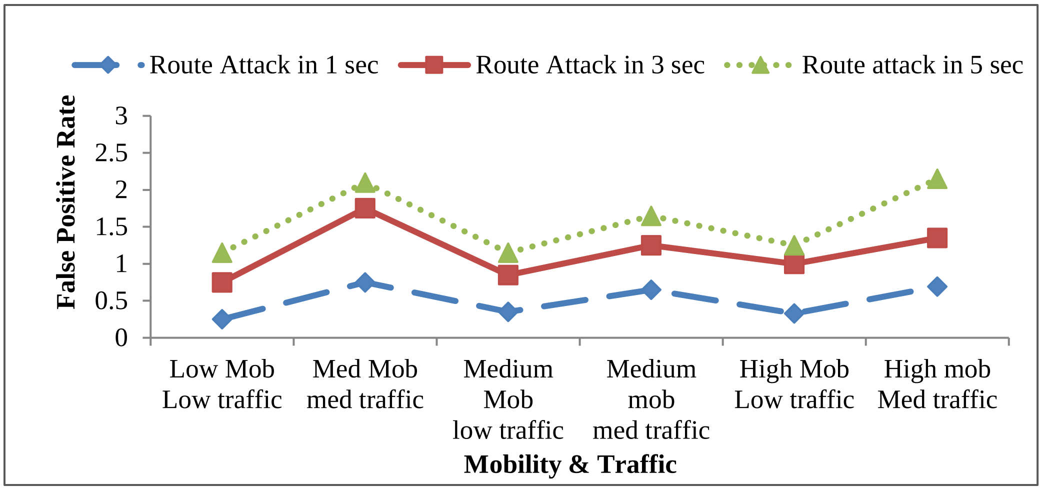

Fig. 13 Route disruption attack execution

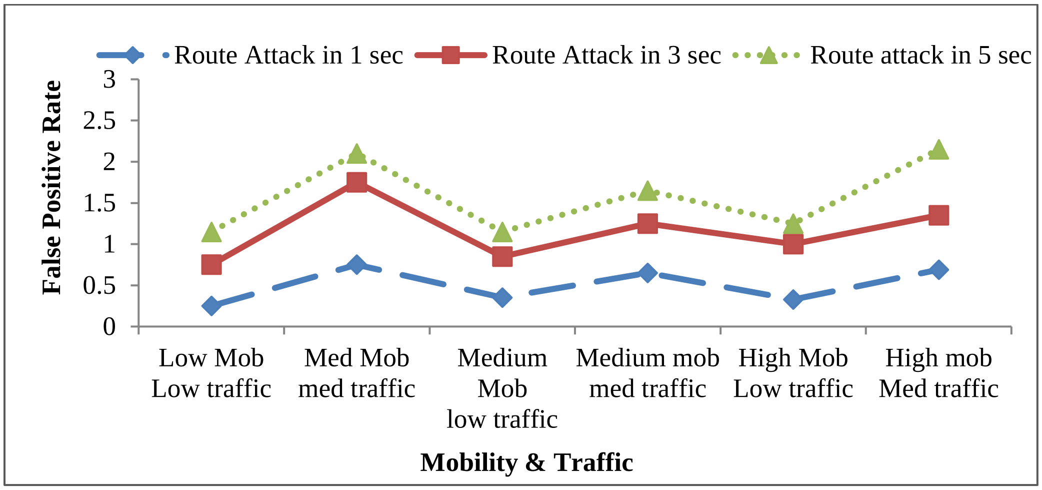

Fig. 14 Adhoc flooding attack execution

The results may be seen in Figure 13, which focuses on the most significant persons. There is a direct correlation between the attacker's dissemination time and the percentage of false positives. The most qualified accuracy detection rate may be compared quickly and easily. Certain persons have a reduced rate of detection as well as a lower FPR among the developing algorithms. These people have a lowered FPR. Both the rate of detection and the FPR are at an appropriate level.

Threshold-based signatures have previously been used to identify resource depletion attacks in WANets. Figure 14 illustrates the effectiveness of the characteristic in using different threshold values on a network featuring medium levels of traffic and mobility. It is demonstrated that its fitness value seems to have a threshold value of 3, upon which it starts to grow, corresponding to the optimal value for this value.

5. Conclusion

Many intrusion detection methods built for fixed wired networks are no longer relevant in this new context. Then, we present the novel intrusion detection & response techniques we are working on for wireless ad hoc networks. In this work, two different IDS approaches are shown. The first strategy involves using the permissive state that varies according to the node's location inside the simulation field. This method is called a Quasi Cluster Head (QCH) algorithm when used with the AODV Routing protocol. The playing area is divided into four quadrants, with a round hole in the middle. The node will have the ability to collect data from other neighbour nodes which are within the radio transmission range of it. The second method, called X-layer IDS, uses Random X-Layer Mobility. Tools to detect ad hoc flooding, route disruption, and dropping attacks directed against WANet are now being developed. The functionality of constantly changing programmes is evaluated using simulated network topologies.

References

[1] Ayoub Alsarhan et al., “Machine Learning-Driven Optimization for SVM-Based Intrusion Detection System in Vehicular Ad Hoc Networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 6113-6122, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Sivanesh, and V. R. Sarma Dhulipala, “Accurate and Cognitive Intrusion Detection System (ACIDS): A Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks,” *Mobile Networks and Applications*, vol. 26, no. 4, pp. 1696-1704, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zainab Ali Abbood et al., “A Survey on Intrusion Detection System in Ad Hoc Networks Based on Machine Learning,” *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)*, pp. 1-8, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Saurabh Singh et al., “Intrusion Detection System-Based Security Mechanism for Vehicular Ad-Hoc Networks for Industrial IoT,” *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 83-92, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Erfan A. Shams, and Ahmet Rizaner, “A Novel Support Vector Machine Based Intrusion Detection System for Mobile Ad Hoc Networks,” *Wireless Networks*, vol. 24, no. 5, pp. 1821-1829, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] R. Srilakshmi, and Jayabhaskar Muthukuru, “Intrusion Detection in Mobile Ad-Hoc Network using Hybrid Reactive Search and Bat Algorithm,” *International Journal of Intelligent Unmanned Systems*, vol. 10, no. 1, pp. 65-85, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Erfan A. Shams, Ahmet Rizaner, and Ali Hakan Ulusoy, “Trust Aware Support Vector Machine Intrusion Detection and Prevention System in Vehicular Ad Hoc Networks,” *Computers & Security*, vol. 78, pp. 245-254, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] R. Santhana Krishnan et al., “Modified Zone Based Intrusion Detection System for Security Enhancement in Mobile Ad Hoc Networks,” *Wireless Networks*, vol. 26, no. 2, pp. 1275-1289, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Satyanarayana Pamarthi, and R. Narmadha, “Literature Review on Network Security in Wireless Mobile Ad-Hoc Network for IoT Applications: Network Attacks and Detection Mechanisms,” *International Journal of Intelligent Unmanned Systems*, vol. 10, no. 4, pp. 482-506, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Shivam Kumawat, Harneet Kaur, and Omdev Dahiya, “An Analytical Study on Intrusion Detection System in Integrated Vehicular Ad-Hoc Network Attacks,” *In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 378-383, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Junwei Liang et al., “A Novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) Based on differences of Traffic Flow and Position,” *Applied Soft Computing*, vol. 75, pp. 712-727, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Rajendra Prasad P, and Shiva Shankar, “Secure Intrusion Detection System Routing Protocol for Mobile Ad-Hoc Network,” *Global Transitions Proceedings*, vol. 3, no. 2, pp. 399-411, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Bandecchi Susan, and Dascalu Nicoleta, “Intrusion Detection Scheme in Secure Zone Based System,” *Journal of Computing and Natural Science*, vol. 1, no. 1, pp. 19-25, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Man Zhou et al., “Distributed Collaborative Intrusion Detection System for Vehicular Ad Hoc Networks Based on Invariant,” *Computer Networks*, vol. 172, p. 107174, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Masoud Abdan, and Seyed Amin Hosseini Seno, “Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET),” *Wireless Communications and Mobile Computing*, vol. 2022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mahendra Prasad, Sachin Tripathi, and Keshav Dahal, “A Probability Estimation-Based Feature Reduction and Bayesian Rough Set Approach for Intrusion Detection in Mobile Ad-Hoc Network,” *Applied Intelligence*, vol. 53, pp. 7169-7185, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Vasaki Ponnusamy et al., “Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks,” *Computer Systems Science and Engineering*, vol. 40, no. 3, pp. 1199-1215, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jose Vicente Sorribes et al., “Energy-Aware Randomized Neighbor Discovery Protocol Based on Collision Detection in Wireless Ad Hoc Networks,” *Mobile Networks and Applications*, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kulkarni Sagar S, and Kahate Sandip A, “Review of A Semantic Approach to Host-based Intrusion Detection Systems using Contiguous and Dis-contiguous System Call Patterns,” *SSRG International Journal of Computer Science and Engineering*, vol. 2, no. 6, pp. 9-12, 2015. [Publisher Link]

[20] Arunkumar Rajendran, Nagaraj Balakrishnan, and Ajay P, “Deep Embedded Median Clustering for Routing Misbehaviour and Attacks Detection in Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 126, p. 102757, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Naveen Chakravarthy Sattaru et al., “Evaluation of Cluster Approach for Detecting Black Hole Attacks in Wireless Ad Hoc Networks using Deep Learning,” *In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 821-825, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] C. Murugesh, and S. Murugan, “Moth Search Optimizer with Deep Learning Enabled Intrusion Detection System in Wireless Sensor Networks,” *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 4, pp. 77-90, 2023. [CrossRef] [Publisher Link]

[23] Jose Vicente Sorribes, Jaime Lloret, and Lourdes Peñalver, “Analytical Models for Randomized Neighbor Discovery Protocols Based on Collision Detection in Wireless Ad Hoc Networks,” *Ad Hoc Networks*, vol. 126, p. 102739, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Leonid Legashev, and Luybov Grishina, “Development of an Intrusion Detection System Prototype in Mobile Ad Hoc Networks Based on Machine Learning Methods,” *In 2022 International Russian Automation Conference (RusAutoCon)*, pp. 171-175, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] S. Kavitha, “Detecting Network Intrusion Based on Machine Learning Algorithms,” *International Journal of P2P Network Trends and Technology*, vol. 10, no. 3, pp. 1-5, 2020. [Publisher Link]

[26] Uppalapati Srilakshmi et al., “A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks, *IEEE Access*, vol. 10, pp. 14260-14269, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Amit Chougule et al., “Multibranch Reconstruction Error (MbRE) Intrusion Detection Architecture for Intelligent Edge-Based Policing in Vehicular Ad-Hoc Networks,” *IEEE Transactions on Intelligent Transportation Systems*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] M. Azath, and Vaishali Singh, “Optimized Convolutional Neural Network Based Privacy Based Collaborative Intrusion Detection System for Vehicular Ad Hoc Network,” *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 2, pp. 143-156, 2023. [CrossRef] [Publisher Link]

[29] B. Murugeshwari et al., “Hybrid Key Authentication Scheme for Privacy over Adhoc Communication,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 10, pp. 18-26, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] S. Kanthimathi, and P. Jhansi Rani, “An Efficient Packet Dropping Attack Detection Mechanism in Wireless Ad-Hoc Networks using ECC Based AODV-ACO Protocol,” *Wireless Networks*, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Adrian P Lauf, Richard A Peters, and William H Robinson, “A Distributed Intrusion Detection System for Resource-Constrained Devices in Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 8, no. 3, pp. 253-266, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[32] Ming-Yang Su, “Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems,” *Computer Communications*, vol. 34, no. 1, pp. 107-117, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[33] Shivam Kumawat, Harneet Kaur, and Omdev Dahiya, “An Analytical Study on Intrusion Detection System in Integrated Vehicular Ad-Hoc Network Attacks,” *In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 378-383, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Mahdi Sadeghizadeh, “A Lightweight Intrusion Detection System Based on RSSI for Sybil Attack Detection in Wireless Sensor Networks,” *International Journal of Nonlinear Analysis and Applications*, vol. 13, no. 1, pp. 305-320, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] Mahendra Prasad, Sachin Tripathi, and Keshav Dahal, “An Enhanced Detection System Against Routing Attacks in Mobile Ad-Hoc Network,” *Wireless Networks*, vol. 28, no. 4, pp. 1411-1428, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[36] Hadi Otrok et al., “A Game-Theoretic Intrusion Detection Model for Mobile Ad Hoc Networks,” *Computer Communications*, vol. 31, no. 4, pp. 708-721, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[37] S. Navya Sai, and K. Kishore Raju, “Improved Privacy Preserving Decision Tree Approach for Network Intrusion Detection,” *International Journal of Computer & Organization Trends (IJCOT)*, vol. 6, no. 1, pp. 55-60, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[38] Ningrinla Marchang, and Raja Datta, “Collaborative Techniques for Intrusion Detection in Mobile Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 6, no. 4, pp. 508-523, 2008. [CrossRef] [Google Scholar] [Publisher Link]