CIT. Journal of Computing and Information Technology, Vol. 30, No. 2, June 2022, 67–83
doi: 10.20532/cit.2022.1005453

A Prey-Predator Defence Mechanism for Ad Hoc On-Demand Distance Vector Routing Protocol

Abiodun Akinwale, Emmanuel Ajayi Olajubu and Ganiyu Adesola Aderounmu

Obafemi Awolowo University, Ile-Ife, Nigeria

This study proposes a nature-based system survivability model. The model was simulated, and its performance was evaluated for the mobile ad hoc wireless networks. The survivability model was used to enable mobile wireless distributed systems to keep on delivering packets during their stated missions in a timely manner in the presence of attacks. A prey-predator communal defence algorithm was developed and fused with the Ad hoc On-demand Distance Vector (AODV) protocol. The mathematical equations for the proposed model were formulated using the Lotka-Volterra theory of ecology. The model deployed a security mechanism for intrusion detection in three vulnerable sections of the AODV protocol. The model simulation was performed using MATLAB for the mathematical model evaluation and using OMNET++ for protocol performance testing. The MATLAB simulation results, which used empirical and field data, have established that the adapted Lotka-Volterra-based equations adequately represent network defense using the communal algorithm. Using the number of active nodes as a measure of throughput after attack (with a maximum throughput of 250 units), the proposed model had a throughput of 230 units while under attack and the intrusion was nullified within 2 seconds. The OMNET++ results for protocol simulation that use throughput, delivery ratio, network delay, and load as performance metrics with the OMNET++ embedded datasets showed good performance of the model, which was better than the existing conventional survivability systems. The comparison of the proposed model with the existing model is also presented. The study concludes that the proposed communal defence model was effective in protecting the entire routing layer (layer 2) of the AODV protocol when exposed to diverse forms of intrusion attacks.

ACM CCS (2012) Classification: Security and privacy → Network security → Mobile and wireless security

Keywords: security, cyber security, survivability, AODV, MANET, OMNET++, network protocols

1. Introduction

Ad hoc On-Demand Distance Vector (AODV) routing protocol is used to select the most suitable route for packet delivery from originating node to destination. Wireless communication media generally rely on routing protocols with multi-hop capabilities to deliver data to desired destinations despite the dynamic nature, limited bandwidth, and low power of the computing nodes of such networks. AODV is a distance vector protocol which normally needs route establishment, which deluges the network with a route request (RREQ) before the route is established. A Mobile Ad hoc Network (MANET) makes the usage of computer systems easy as it establishes computer network without engaging any infrastructure [1]. Interestingly enough, MANET employs AODV routing protocol as the official protocol for the network communication. However, the protocol is reactive, which implies the routes are generated only when required. Traditional routing tables are employed to predict the viability of a route from time to time, by using predefined sequence numbers to predict whether the route's information is up to date and to avoid any form of looping [2]. Networks that use AODV routing protocol for communication, however, face extremely difficult security challenges [3, 4], such as denial of service (DoS) and distributed denial of service (DDoS) when multiple nodes are involved, due to wireless, infrastructure-less, dynamic topology, limited power and mobility nature of the net-

work on the one hand and also because AODV is a widely deployed routing protocol for mobile wireless networks on the other hand. These attributes make the network vulnerable to diverse kind of cyber-attacks that occur in the form of network intrusions [5, 6].

AODV cyber intrusion takes place in the realms of the routing layer. An intrusion is a premeditated attempt to compromise the confidentiality, integrity and availability of a network resource [7]. Intrusion, therefore, interrupts, intercepts, and modifies normal information and communication flow in a network as well as the fabrication of false data. The result of most attacks in this network is a DoS and when it involves many collaborating systems, it becomes a DDoS. Other frequent attacks on the network include wormhole attacks, which forward the routing control message to another colluding node usually using a high-gain directional antenna communication link to prevent the completion of a routing discovery process. The colluding nodes create a tunnel in-between them and deceive targeted nodes that they are just one-hop away by virtue of the high-gain directional antenna, thus diverting network traffic into the tunnel [8]. On the other hand, black-hole attacks use the capability of an intruder node to present itself as the shortest route to destination nodes after receiving respective route requests (RREQs) from several source nodes [9]. In another form of black hole attack, the attacker randomly drops packets in the network, which is termed grey hole intrusion. Flooding intrusion is a denial-of-service attack aimed at AODV protocol that hijacks the route discovery phase of its operation. The two types of flooding attacks (RREQ flooding and DATA flooding) hijack existing routes in a wireless network and flood it with an abnormal number of RREQ and data packets to non-existent IP addresses [8]. Most attacks occur at the network layer of the TCP/IP protocol stack where AODV is actually deployed. Already, many algorithms have been developed for intrusion detection and prevention for AODV protocol layer, but yearly statistics of attacks reveal an increase in the technical knowledge of intruders who constantly develop innovative schemes or algorithms for new/undocumented attacks. The implication is that no amount of system hardening can make a system completely invulnerable to attacks.

Literature has explored the biological traits to design algorithms for network security, such as [10]. The model proposed in this work is different, in that it considers the dynamic topology of the network and the volatility of the nodes in the network. Thus, this paper presents a prey-predator model for AODV security that enables wireless networks (MANETs, WSNs and IOTs) to keep on delivering data to a stated destination even when there are intrusions. This is referred to as survivability of a system. Survivability model empowers a system to continue to consistently deliver on its mandate without disruption, even when there are intrusions, network failures, or accidents [11]. The model encapsulates the entire integrity and reliability of a system [12]. Current survivability models for AODV protocol use conventional or standard security solutions. Most of these models deploy generic algorithms that fail to address the dynamic or morphing nature of wireless attacks [13]. Bio-inspired survivability algorithms [14] potentially provide better solutions but are very scarce in literature. Techniques using prey-predator solutions are virtually non-existent, despite their potentials for dynamic and robust defence capabilities. The need for AODV systems to have the ability to fulfil their stated missions in the presence of any type of attack or failure, using techniques analogous to animal prey-predator systems, form the basis for this work. Biological organisms have some characteristics which can be very useful for wireless networks defence. The biological characteristics are often used for survivability of these organisms in the presence of their predators [15, 16]. This is employed and adapted in this work, where an adaptive or self-tuning prey-predator defence method is used to design a survivability solution for AODV routing protocol at the network layer of MANET to ensure optimum throughput at all times. The next section discusses the existing work in this body of knowledge. The theoretical work and the proposed model are presented in sections 3 and 4, respectively. Section 5 elucidates the performance evaluation of the model, while section 6 presents the simulation results. Section 7 concludes the paper.

2. Related Work

Many researchers have proposed models to address the security weakness of AODV routing protocol. The developed solutions either mitigate a single attack or group attacks in a particular layer of the network. In quest for solution to the problem at hand, Bello and Lambain [17] proposed a scheme for sinkhole detection and mitigation in wireless sensor networks using AODV routing protocol, because sinkhole is one of the most destructive attacks on WSNs due to their many-to-one connectivity situation. This means an intruder can pose as the base station destination and begin to sink data and control packets intended for the authentic base or controller station. To mitigate this type of activity, the authors introduced delay-per-hop-indicator (Delphi) in addition to geographical detection based on the fact that a malicious node will need to change the delay time (time needed by receiver to receive data after RREP has been sent to source). Delphi calculates the expected delay per hop using the geographical location coordinates of a suspected node from the source, and compares it with its neighbor, and then indicates malicious activity from a node when a false Delphi is forwarded by the node. The offending node is then eliminated from the network. The drawback to this method is the possibility of a wrong Delphi threshold being chosen, which can generate a lot of false positives. According to Amish and Vaghelain [18], AODV security was enhanced by detection and prevention of wormhole attacks when multipath routing method was employed in WSNs. By using more than a single path for routing, the round-trip time (RTT) for each node is divided by the number of hop-counts to calculate the threshold value. Individual RTTs are then compared with the threshold value. If a node's RTT is less than the threshold and the hop count is equal to two, then a wormhole activity is detected. This method is only useful when there are multiple paths to the destination node. Also, the condition that the hop count must be two to determine a wormhole activity is suspected, because in some cases, hop count between two cooperating malicious nodes present themselves as just one hop count.

In the work of Ghayval *et al.* [19], the authors presented a model for efficient detection and mitigation of wormhole attack in MANETs using an advanced AODV approach. This was done by calculating the tunnelling time taken between two normal nodes and an average threshold value is set and compared with individual tunnelling times of nodes in the network to detect a wormhole activity. Once a malicious activity is detected, a digital hash chain is used to block the offending link in the network. The key issue in this work is the process of generating a correct tunnelling time value. If this is wrong, then the entire process has a suspicious value. Following the same line of thought, Prakash *et al.* [20] used a technique that employed election for leadership to develop an algorithm that uses coordination to mitigate the wormhole attack. A wireless algorithm was designed to elect the leader; this is due to the dynamic nature of MANET. There are six steps involved in the leadership election algorithm, as an interested reader can read in [20] for more details. The leader's responsibility is to detect the path that is vulnerable, which is the wormhole that is a path with wormhole channel. Every node on the network will have to be registered. For a new node to join the network, registration is mandatory. When a coordinator leaves, an election has to take place to elect another leader or coordinator. The main duty of the coordinator is to trace any paths that serve as wormholes in the network and if it is a single path, the node is immediately isolated from the network. The result of the experiment showed the effectiveness of the proposed model. The throughput value for 100 nodes when there is no attack was 90.02, when under attack the throughput was 58.32, and while the algorithm prevented the wormhole attack the throughput was 89.85. The results imply that prevention of a wormhole attack is better than mitigating the attack when it has occurred.

Tahboush and Agoyi [21] improved on the work of [18] by adding packet delivery ratio and transmission range value to RTT in the calculation for the required threshold value to use in detecting malicious activity in AODV-based networks. Though the work provides better threshold value to reduce false positives, the overhead of additional metrics may offset the gain [21].

A survey of existing routing survivability techniques as of 2013 was carried out by Ahmed *et*

al. [8]. The work classified the schemes into three main initiatives of authentication, path selection and attack location with detection. This served as a future research direction for survivability systems. In another paper, Joshi and Biradar [22] used MANET head nodes to identify malicious nodes and improve packet delivery in AODV-based networks. This was done by firstly initiating a fake packet transmission to establish the efficiency of delivery from source to destination. Thereafter, a MANET head node was appointed to identify trusted nodes by assigning trust levels to them. The trust factor generated from assigned trust levels was used between neighbour nodes to identify malicious nodes and isolate them from the network thus improving packet delivery. The challenge here is network redundancy during testing and before authentic transactions start, as this process can slow down network performance. In a similar manner, Ran *et al.* [23] proposed a blockchain technology for multipath discovery in MANET. The authors focus their work on improving quality of service (QoS), assuming that this will have a direct effect on the security of the system. On one hand, QoS rarely affects intrusion and on the other hand, the blockchain technology used cannot effectively cope with the dynamic nature of MANET. Any algorithm that will work on MANET security must be scalable.

The core contribution of the work of Bondada *et al.* [24] is the ability to predict the value of trust through the comparison of log reports of the node with a generated ID sequence of the nodes. As the routing protocol which arranges its routes in advance from the most recent paths is reactive, updating the route path to destination is easy, but the malicious nodes make this functionality highly predicable. In this work, the trust value is calculated using a cryptographic algorithm, energy evaluation, the rate at which packet are delivered, nodes mobility and location. Nodes with the highest trust are permitted to transmit data, which makes the route trustworthy and reliable. The intrusion detection system uses alarm to identify attacks and then launches the intrusion prevention mechanism of the model. This reduces the attacks rate in the system far more than the existing models. The throughput and the packet-delivery ratio of the proposed model is better than the existing models.

The use of machine learning is making waves in many fields of study. A machine learning algorithm was proposed for intrusion detection by Sultanuddin and Hussain [25] for MANET. The algorithm is based on anomaly detection with a classified intrusion detection system (IDS) using reinforcement learning. Decision tree learning was used to improve precision of the model. The model is also based on the agent mechanism; the cluster head / IDS agent performs intrusion detection activities in the system. This provides the patterns of behavior of the individual node on the network. Involvement of any node anomaly behavior gradually degrades network performance. The model has improved performance over the existing model but may be too complex for real-life implementation. The model proposed by Tesfay *et al.* [26] initiated the detection and prevention of sybil attacks in MANET. A sybil attack occurs when a malicious device decides to distribute its identity with other sybil nodes to deceive a legitimate device on the network. The sybil detection and prevention model performs some analysis that is based on past records of the device and compares it with present analysis, which eventually initiates the blocking in a real-time scenario. The model was developed in NS-2 and normal metrics for evaluation of MANET performance were applied. The proposed model's performance was 90.7% with respect to detection accuracy and a 97.85% true positive rate. Abbas *et al.* [27] presented a model that theoretically analyzed the survivability of MANET routing protocol (AODV) under DoS attacks without any intrusion detection system. The study examined the response of reactive and proactive AODV under DoS attack and used this to determine the survivability of AODV under DoS attack. Also, Talukdar *et al.* [28] carried out a performance analysis of AODV protocol when under the black hole attack. This seems to be the closest work to this study; therefore, the performance of the proposed model is compared with this existing model later on in the paper.

All the models reviewed above deploy algorithms that either target a specific type of attack or develop an algorithm that will have an impact on security of AODV but fail to address the morphing capability of that type of attack. This work proposes a model that is dynamic and able to morph with the type of attack encountered in

AODV at the network layer of MANET. It also ensures that any network based on the protocol is able to deliver packets consistently to the required destination without any alteration in the face of attacks.

3. Theoretical Framework

The theory supporting this research work is the prey-predator model. The dynamics of prey-predator is used to depict 1-MANET 1-attacker system which is used to explore MANET and intrusion attacks. The mathematics behind the survivability model is developed, with the service delivery is presented in this section.

3.1. Mathematical Model of Survivability

The key issue in prey-predator ecology is the population. That is, how the presence of predators affects the population growth rate. The rate of growth of the population of a species determines the survivability of that species. Also included is the per capita growth rate of individuals in ecology. The major concern in MANET survivability design is the quality of service (QoS) in the network, which encapsulates availability, integrity, tolerance, timeliness, and others. This implies that the presence of intruders affects link quality. The capability of maintenance of good service delivery despite attacks determines the survivability of the network. The individual service delivery of nodes in a MANET is equally important.

3.2. Modelling Link Quality or Service Delivery

The link quality rate (change in quality of service in a network over time) for a MANET N, and service delivery rate a of individual nodes in the network can be expressed as:

$$\frac{dN}{dT} = aN \tag{1}$$

The logistic equivalent of equation (1) includes the element of boundary or maximum carrying capacity K of the entire MANET. The equation then becomes:

$$\frac{dN}{dT} = a\left(\frac{K-N}{K}\right)N = aN\left(1-\frac{N}{K}\right) \tag{2}$$

where N is the present number of nodes in the network and K the total bandwidth of the network channel, as shown in (2).

3.3. One-MANET One-Attacker Model

Using the methods proposed in [29] and [30], equation (1) is modified for a 1-MANET 1-attacker system. For a MANET size N and with the intrusion type P, the equation becomes:

$$\frac{dN}{dT} = aN - bNP \tag{3}$$

$$\frac{dP}{dT} = qNP - sP \tag{4}$$

where,

P = no. of attacker nodes
N = no. of active normal nodes
T = time taken during attack
a = growth rate of normal active nodes
b = attack rate by malicious nodes
s = rate of neutralising intrusion attack
q = efficiency of intrusion attack.

Applying the maximum capacity ceiling K of the network, equations (3) and (4) become:

$$\frac{dN}{dT} = aN\left(1-\frac{N}{K}\right) - NPR \tag{5}$$

$$\frac{dP}{dT} = PG(N,P) = P(qN - s) \tag{6}$$

An extension of the above to include two MANET species (N and M), where AODV intrusion species P probabilities' components U and V are adapted from [29], gives equations (7)–(9), as follows:

$$\frac{dN}{dT} = N\left[r\left(1-\frac{N+M}{K}\right) - \frac{aU_nV_nP}{1+aU_nN\left(T_e+VT_l\right)+aU_mM\left(T_e+V_mT_l\right)}\right] \tag{7}$$

$$\frac{dM}{dT} = M\left[r\left(1-\frac{N+M}{K}\right)- \frac{aU_m V_m P}{1+aU_n N\left(T_e+U_n T_l\right)+aU_m M\left(T_e+V_m T_l\right)}\right] \quad (8)$$

$$\frac{dP}{dT} = P\left[\frac{\varepsilon a\left(U_n V_n N+U_m V_m\right)}{1+aU_n N\left(T_e+V_n T_l\right)+aU_m M\left(T_e+V_m T_l\right)}-d\right] \quad (9)$$

where the population of active nodes for the two MANETs are N and M, respectively, and the population of the active nodes or threats is P, the rate at which threats are released is a, while the probability of an attack on nodes in MANETs M and N respectively is (U_m, U_n). The probability that a node or route i is successfully destroyed after attack is V_i. Maximal per capita growth rate of nodes / links in MANET is r, while the time taken during early (pre-attack) defence operations T_e. The time taken during post-attack defense operations is represented by T_l and the efficiency of a successful attack operation by an intruder is Ɛ.

4. Proposed Prey-Predator Model Design

The prey-predator model proposed in this work is derived from communal animal defence. This is the strategy of a group of prey-animals (analogous to vulnerable wireless networks) collaboratively working together to survive and frustrate or prevent attack in the group. The more the number of preys (nodes or routes) in the network, the less is the possibility of the attack to be successful. This strategy bodes well for network scalability.

The nearest (1-hop neighbor) nodes are collaboratively employed in the design to inflict most damage to attackers. Table 1 compares communal defense with the MANET/WSN equivalents.

4.1. Communal Defense Algorithm

The communal defense model consists of launching a collective defense by bombarding the intruder with HELLO & RREP-ACK packets. The bombardment is only done for a regulated time (to prevent network flooding) by 1-hop neighbor nodes to the attacker in response to SOS packets sent by the victim to the network. The algorithm used to achieve this is shown in Figure 1.

Table 1. Communal prey defense and MANET equivalence.

Communal Defense Method	AODV Network Equivalent
Prey type	MANET
Single prey	One node
Prey population	No. of AODV routes / no. of nodes
Predator	Intrusion type
Predator population	Route disruption capacity or magnitude of intrusion / no. of attacker nodes
Cost of hibernation	Cost of defense (possession + usage)
Nearest neighbor	One-hop neighbor nodes
Inflicting damage	Data flood to intrusion node
Collaborative preys	Collaborative one-hop nodes

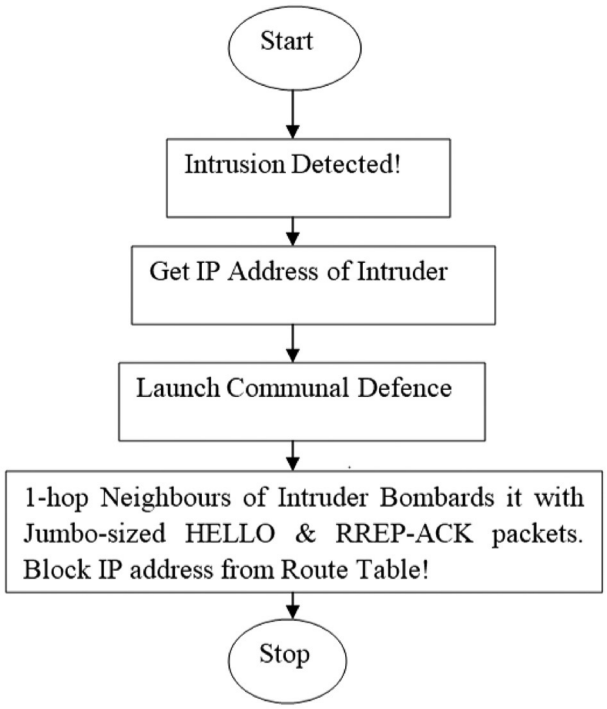


Figure 1. Communal Defense Algorithm for AODV.

This is largely a post-attack type of defence. Once an intrusion is detected, the victim node sends an encrypted SOS message including the IP address of the attacker to other network nodes (using the dynamic routing table) that are 1-hop away from it, but excluding the attacker. These 1-hop neighbour nodes then cooperatively flood the malicious node with rapidly generated HELLO and RREP-ACK packets for a specified time. This renders it inoperable and runs down its resources. The attacker is then blocked from the network. The victim node rescued during the bombarding period is able to forward packets to the desired destination.

4.2. Intrusion Detection System

A robust IDS is fundamental to the efficiency of a survivable system. This is because, if an attack cannot be detected, there is no way to prepare for a mitigation, countermeasure, or survivability process.

There are three broad categories of intrusion detection systems, namely: signature-based IDS, which use patterns of malicious bytes to detect attack; anomaly-based IDS that studies the behavior of a network or a node; and classify normal from abnormal behaviors according to a set of criteria determined by the developer and hybrid IDS, which combines the attributes of signature-based and anomaly schemes. This work uses a novel technique of detecting intrusion, called Protocol Surveillance Intrusion Detection System (PS-IDS). Our intrusion detection system is based on the fact that TCP/IP mobile network communication uses a set of standard protocols or rules that a normal or non-malicious user adheres to for effective and acceptable communication to take place between devices at the network layer. Since the goal of intrusion attacks is to break rules or violate protocol specifications, an intrusion is therefore a violation of or non-adherence to acceptable thresholds for a protocol.

4.3. Communal Defense for AODV

PS-IDS intrusion detection was deployed to monitor the weak points vulnerable to attack in the AODV protocol, as depicted in Figure 2. An intrusion is detected when at least one of the following three cases occurs: (i.) the numbers of route request (RREQ) is greater than the maximal allowable RREQ in the AODV routing process. This is the safety net embedded in AODV to prevent flooding. Only a criminal system violates this security threshold. (ii.) the hop number of the destination node is less than the hop number of the RREQ sent by the sender. This is because the hop number of the receiver must be greater or equal to the hop number of the RREQ. (iii.) the receiver is not sending the acknowledgement of the route reply (RREP). A sinkhole node, for example, never sends (RREP-ACK) back to the source. All the above protocol aberrations correspond with symptoms of intrusions, such as sinkhole, black hole, DoS attacks, and others. The entire algorithm describes the communal defense protection for the network. As soon as intrusion is detected in any part of the AODV routing phase, the following steps are initiated one after the other:

1. The IP address of the malicious node(s) is detected from the AODV routing table using its destination address, netmask, gateway, interface, and metric number as parameters.
2. One-hop neighbors of the offender are forced to bombard it with maintenance

packets (HELLO & ACK) for a limited time determined by the Optimum Exploring Algorithm (OEA).

3. OEA ensures that the flooding process is balanced between normal network activity and the depletion of the offender's critical resources.
4. The offender's MAC address is blacklisted to prevent spoofing.
5. The offending IP address entries are removed from the routing table.
6. Normal network activities continue.

Any transmogrification after bombardment of a stubborn offender would take some time during which data transfer must be taking place from source to destination. For real-time multimedia applications, PS-IDS ensures that any further attack at any other part of the protocol is dealt with the same way, thus offering real time protection for the entire layer.

5. Model Evaluation

The complexity of the model simulation required the use of OMNET++ and MATLAB simulation tools. OMNET++ was the main tool for protocol and parametric simulation, while MATLAB was used to simulate the mathematical model. The results of the two tools were then cross validated.

5.1. Performance Metrics Definition

The four performance metrics used to evaluate this model were: network load, network throughput, packet delivery ratio and end-to-end delay. The metrics were selected to benchmark the proposed model fused into AODV with the existing AODV without the security mechanism. This approach was used to show the level of load added by the security model to the protocol.

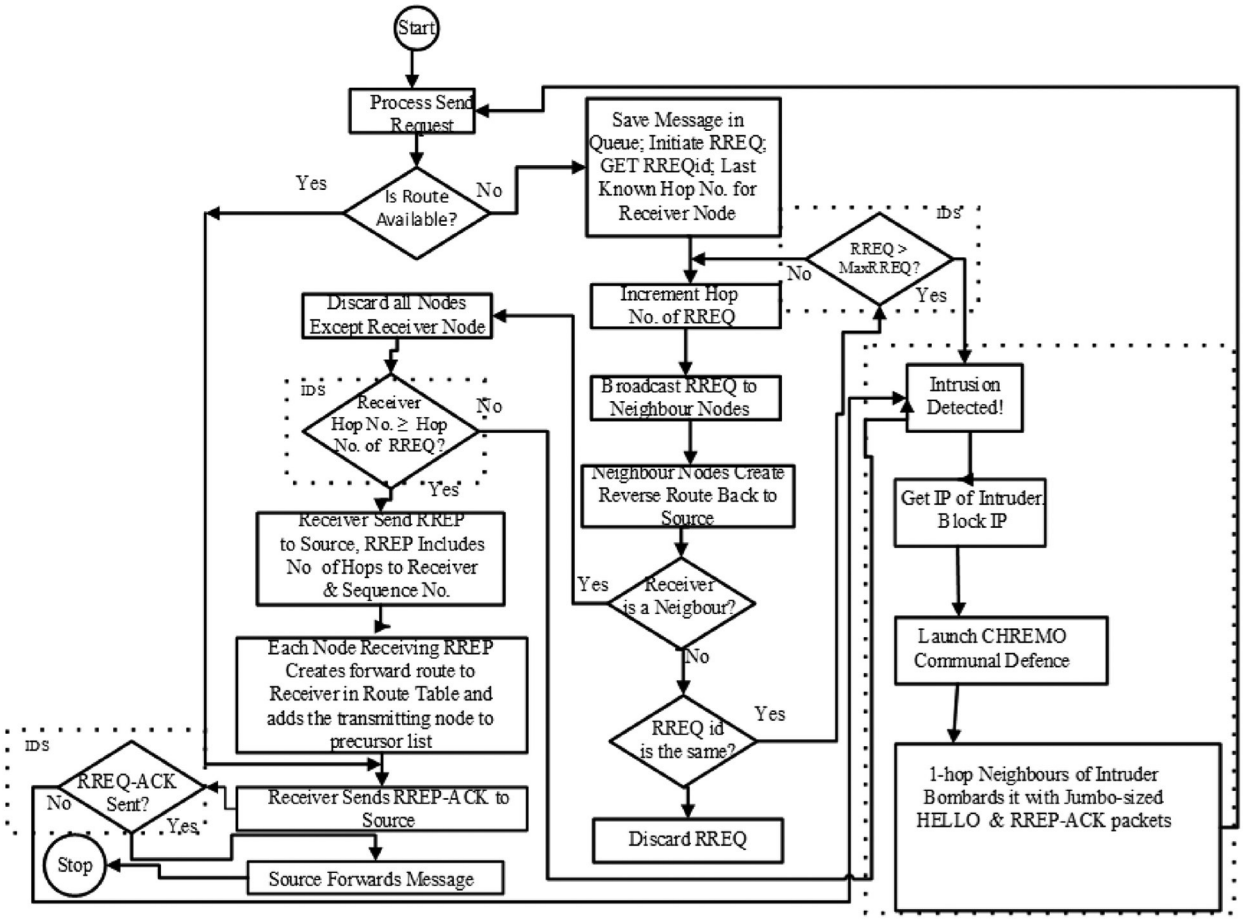


Figure 2. Algorithm for network communal defense of the AODV protocol.

5.1.1. Network Load

Network load measures the amount of traffic generated during the discovery and maintenance processes of a protocol, for example, the total number of Hello, RREQ, RREP and RERR packets in the protocol. Factors contributing to high overhead include the size of network – which is important for multiple hops from source to destination, and the mobility rate, as more links are made and broken arbitrarily when mobility increases. The lower the load or overhead, the higher the throughput of the network and the more efficient the protocol.

In respect to AODV, the total routing overhead is the summation of all the content involved in the communication. It is given as follows:

$$\begin{gathered}\text{Routing Overhead} = \\ \text{Total no. of HELLO pkts} + \\ \text{Total no. of RREQ pks} + \\ \text{Total no. of RERR pkts} + \\ \text{Total no. of RREP pkts}\end{gathered} \tag{10}$$

5.1.2. Network Throughput

The throughput is the ratio of the total amount of data received from a sender to the time it takes for the receiver to get the last packet. It is expressed in bits per seconds or bytes per second. A high network throughput is desirable for protocols; however, one factor that affects throughput in AODV routing is mobility – the higher the mobility, the lower the throughput. This is because a higher mobility leads to frequent topology changes, which in turn affect data being sent to different destinations.

5.1.3. Packet Delivery Ratio

Packet delivery ratio is measured by the quantity of the data delivered to the destination divided by the amount of data packets sent by the source. It effectively measures the loss rate and represents the maximum throughput a protocol may achieve. A high packet delivery ratio is desired in any efficient protocol. Here also, mobility must be factored in. Generally, packet delivery ratio is express as:

$$\text{Packet delivery ratio} = \frac{\text{Total packets delivered}}{\text{Total packets sent}} \tag{11}$$

5.1.4. End-to-End Delay

The network end-to-end delay is defined as the average time a packet routes its path from source to the destination. The time taken includes time spent on queue buffers, transmission time, and other delays introduced by routing activities. Different applications have different levels of tolerance for delays. While some applications 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; namely, the higher the rate of mobility, the higher the delay incurred by the network.

5.2. OMNET++ Simulation Experimental Setup

OMNET++ was configured to determine the performance of AODV based on the specified parameters. The INET framework module suite in OMNET++ was employed for the simulation because of the vast set of models it possesses for MANET and the ability for a user to customise the output vector statistics as required. The INET contains various frameworks that can simulate other networks. ManetRouterNetwork Description (NED) was selected because it is the tool developed mainly for MANET simulation. In this work, three classes of scenarios were modeled and simulated. Each setup was used to model (i.) a normal protocol (ii.) the protocol under attack and (iii.) the protocol with a defence countermeasure. The parameters for the experimental setup in OMNET++ are shown in Table 2 and the simulation setup is shown in Figure 3.

Table 2. Parameter settings for the AODV protocol in OMNET++ simulation.

Parameter	Value
Simulation time (s)	3600
Number of nodes	100
Simulation area (m)	500 × 500
Sending interval (s)	0.1
Protocol	AODV
Node speed (m/s)	2
Data rate (Mb/s)	15
Transmit power (W)	2.0 mW
Number of channels	10
Carrier frequence (Hz)	2.4/5 GHz
Traffic model	TCP
MAC protocol	IEEE 802.11g
Packet size – CBR (bytes)	10

5.3. MATLAB Experimental Setup

This is a post-attack defence mechanism where 1-hop neighbour nodes are triggered to cooperatively flood a malicious node with useless jumbo packets for a specified period of time in order to render the attacker useless and run down its resources after being blocked from the network. The victim node is rescued by redirecting its packets through an available 1-hop neighbour to their destination. The parameter settings for the simulation in this environment are:

$$\text{Cost of defence } \{C_e, C_l, C_{le}\} \qquad (12)$$

Where the cost of possessing early defence is C_e, the cost of possessing late defence is C_l, and the total defence usage cost to escape and survive is C_{el}.

The communal defence operates as a post-attack mechanism, however, every MANET node (m or n, where m is an active, and n is a passive node) is designed to possess both pre-attack and post-attack defence components, though both may not be used at the same time. Hence, the possession cost of both defences will still be incurred. All costs are relative to the cost of node destruction, which cannot exceed 1. This work assumes a hostile environment, where attackers are persistent in their malicious operations as well as a mission-critical financial application

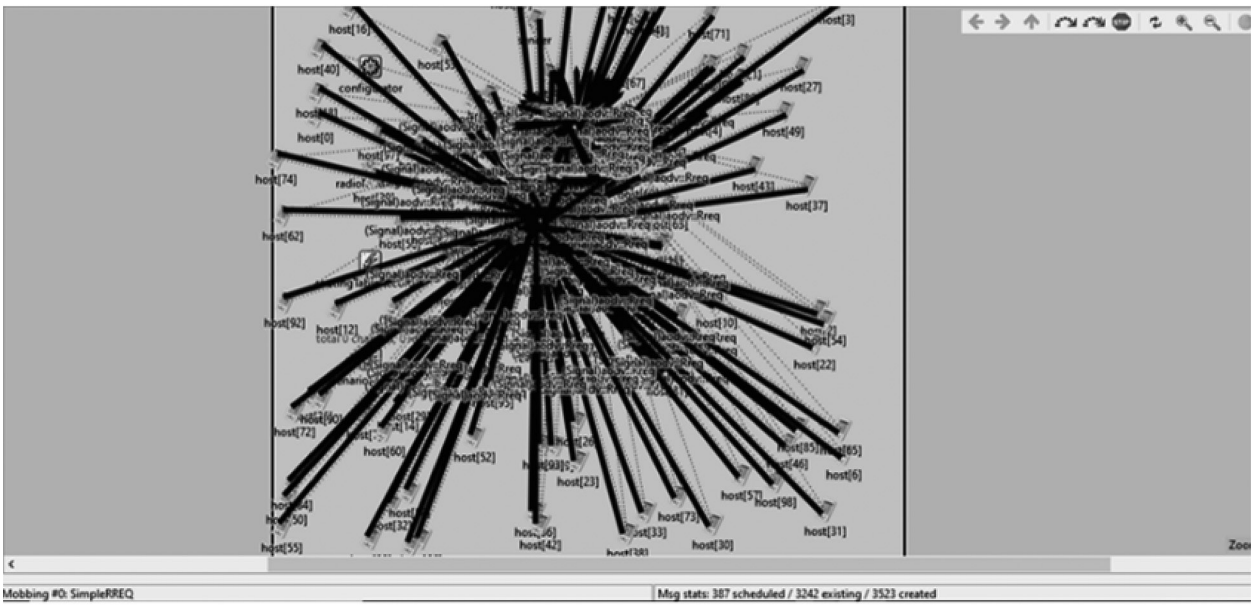


Figure 3. Simulation setup for the AODV protocol with communal defence.

aimed at delivering its mandate in a timely fashion. This implies that the rate of encounter a of a MANET with malicious nodes is high, as opposed to a friendly environment. Each node's encounter rate with attackers is given by equation:

$$a_i = \left\lfloor \frac{aP}{1 + aU_n N\left(T_e + V_n T_l\right) + aU_m M\left(T_e + V_m T_l\right)} \right\rfloor, \tag{13}$$

where a_i is a_n or a_m.

The maximum carrying capacity K is determined by the bandwidth and stream data rate available to nodes for routing or data transmission. Using the 802.11n protocol with a bandwidth of 20 Mhz and a maximum data rate of 288 Mbits/s available, the maximum carrying capacity will be 250 nodes for an effective throughput, by allocating 1 Mbits/s for data transmission assuming that all nodes transmit simultaneously. The number of mobile nodes in the master MANET (N) is 100. In this defence module, the second MANET (M) is redundant, and the number of active nodes is assumed to be 1. This implies that though the second MANET is a backup, it is in a wait state but not dead. The number of intruder nodes is determined by the type of attack. For this module, the network is exposed to a wormhole attack, which requires two colluding nodes intercepting and dropping packets in a network. The probability of attacking a MANET node U_n or U_m that deploys the communal defence is a bit higher than the pre-attack methods. The probability that a node/route n or m in MANETs N or M respectively is successfully destroyed after attack (V_n, V_m) is however very low for communal defence. The growth rate r is a fraction corresponding to the difference between the total numbers of active nodes in a MANET minus the number of dead or inactive nodes divided by the total number of active nodes before attack. More details on the communal defence simulation parameters are given in Table 3.

Table 3. Communal defence simulation parameter settings.

Parameters	Value
Population of active nodes or route links in MANET 1 (N)	100
Population of active nodes or route links in MANET 2 (M)	1
Population of malicious nodes or threats (P)	2
Encounter rate of intruder with MANET (a)	0.8
Probability that an intruder node attacks a node i when within range (U_i)	0.1
Probability of attack on nodes in MANETs M and N, respectively (U_m, U_n)	0.1
Probability that a node or route i is successfully destroyed after an attack V_i	0.1
Probability that nodes / routes m and n in MANETs M and N, respectively, are successfully destroyed after attack (V_m, V_n)	0.1
Maximal per capita growth rate of nodes / links in MANET (r)	0.55
Maximum carrying capacity of the two MANETs N + M (K)	250
Time taken during early (pre-attack) defence operations (T_e)	0.05
Time taken during post-attack (late) defense operations (T_l)	3
Efficiency of a successful attack operation by intruder (Ɛ)	0.01
Decay rate of the intrusion attack (d)	0.8
Cost of early defence by node i (C_{ei})	0.08
Cost of late defence by node i (C_{li})	0.35
New maximal per capita (link quality) growth rate r for node i with possession cost for ($r \cdot (1 - C_{ei} - C_{li})$)	0.55
Defence usage cost to survive and escape ($C_{eli} = C_{ei} + C_{li}$)	0.43

6. Results and Discussion

This section discusses the simulation results of the proposed model for the purpose of analysis. There are two sections; the first one covers the MATLAB simulation results and the second one covers the OMNET++ simulation results.

6.1. Mathematical Model Simulation Results in MATLAB

MATLAB was used to test the mathematical engine of the entire framework. The goal here was to test the mathematical behaviour of the AODV communal defence system. Classical Lotka-Volterra models normally yield sinusoidal waveforms in the face of attack [16]. This is unacceptable for a mission-critical application on the networks. For computer networks, this implies the following:

1. At time t = 0 of an attack, the intruder and victim node on a network have zero throughput.
2. As time elapses, the attacker gets stronger, and the resources of the victim node gets continually depleted.
3. At time t = maximum, the attacker takes over the entire node or network deploying its maximum payload.
4. After t = maximum, the victim node is 'overpowered', but the decline of the attacker begins since it has no other resources in the victim to attack.
5. As the attacker withdraws its payload, the victim resumes operation.
6. Procedure goes back to (1) above.

The above model scenario is unacceptable, since there is no survivability of the network nodes.

Further adaptation of the basic mathematical model to include elements of attack probabilities, early and late defense methods, is necessary. An acceptable model should yield an asymptotic throughput and cascading attack remission when a defense mechanism is activated. Hence, the results in this section show that when defence capabilities are coupled with Markovian attributes and, when factoring in the maximum capacity of a network, a stable system denoting survivability is achieved. In this study, there are two types of MANETs employed. MANET *N* is the active network while MANET *M* serves as a backup for the active MANET at time t = 0 (reference when there is no attack), when MANET *N* throughput is 100 units, and the backup MANET *M* is 15 units. The intrusion magnitude is 10 units. On deploying the communal defence, MANET *N* increased steadily to 230 asymptotically, MANET *M* equally increases throughput to 22 units and the intrusion decreased to 0 units within 2 seconds, as shown in Figure 4.

The figure shows the expected result, namely that a modified classical prey-predator system

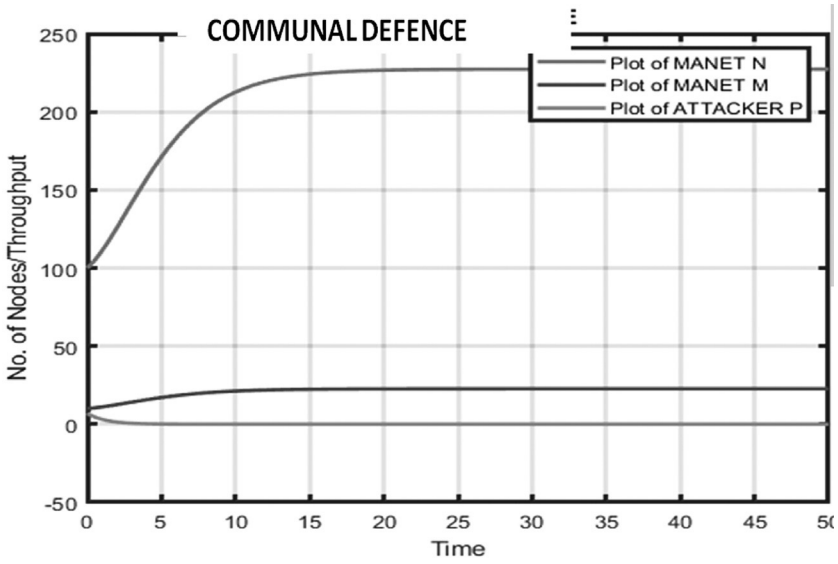


Figure 4. Simulation result for communal defence.

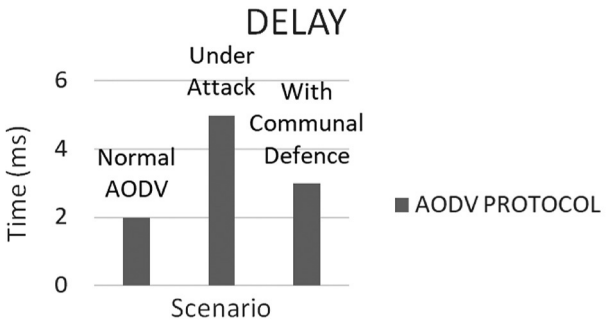
can model survivability behaviour of network species under attack from network intrusion species.

6.2. OMNET++ Simulation Results

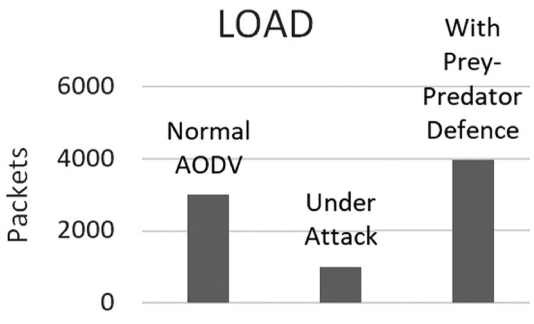
OMNET++ was used to simulate the behavior and responses of the AODV protocol for the deployment of the communal defence scheme against attacks. Four measurement criteria were employed for the evaluation of the algorithm. The result of the experiment is presented in the following sections. The number of nodes involved in the simulation during the experiment was 100. Constant bit rate (CBR) was used for data transfer among the nodes in MANET environment. The wireless standard was IEEE 802.11g with different data (bits) and transfer rates for the layer. The dimension of the simulation area was 100 x 100 square meters. The attack models for this routing layer were sinkhole, black hole, and DDoS attacks. The results of the collaborative or communal mechanism shows a network delay of 3 milliseconds, a routing load of 3970, a delivery ratio of 80% and a throughput of 700 packets/second.

Using maximum throughput, low delay, low load, and maximum delivery as measurement criteria, communal defence performed better on layer 2 (AODV) of the protocol stack when compared with the same network without the deployment of the predator-prey communal defence system.

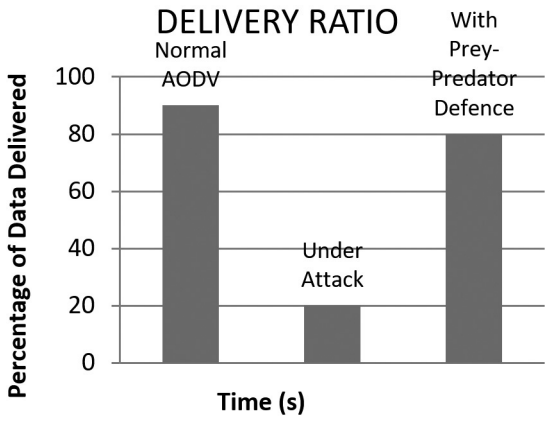
The simulation results show that the pre-predator model has a relatively lower delay when compared with the normal AODV under attack, as shown in Figure 5 (a); nevertheless, the load incurred in the prey-predator model is slightly higher than AODV under attack, as presented in Figure 5 (b). The normal AODV delivery ratio under attack is far lower than the delivery ratio of the pre-predator model, as presented in Figure 5 (c) and the throughput of the AODV under attack is also far lower than the pre-predator model as depicted in Figure 5 (d). It is clear from the simulation results that the proposed model has an impressively better performance than AODV when subjected to the same condition.



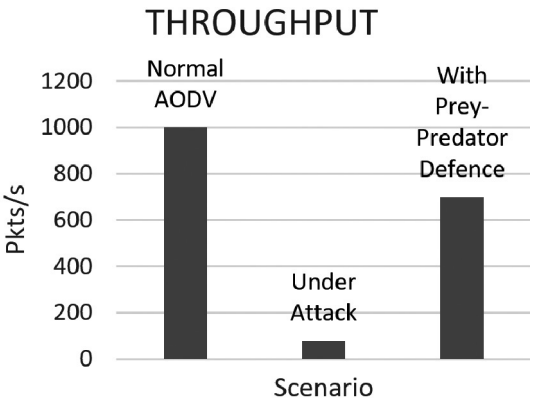
(a) The delay of the system.



(b) The load incurred in the system.



(c) The delivery ratio of the system.



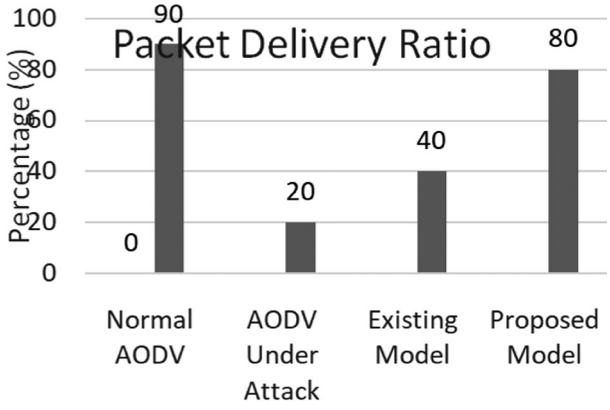
(d) The throughput of the system.

Figure 5.

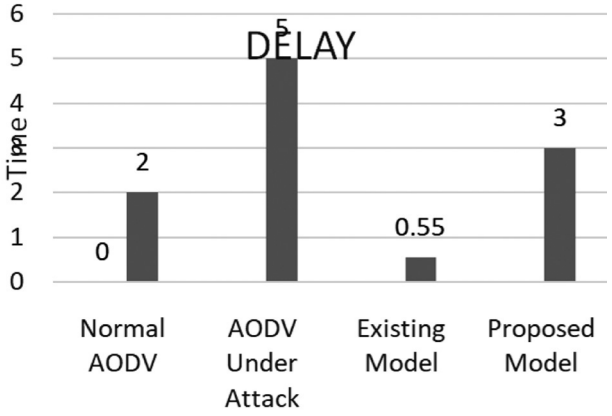
6.3. Performance Comparison of the Proposed Model with Existing Model

The closest model to the proposed model found in the literature is the one by Ibrahim *et al.* [28]. The results of the proposed model were compared with the existing model using the performance metrics common to the two models which are packet delivery ratio, load, and delay. Figure 6 (a), (b), and (c) presents the results of the comparison of the two models.

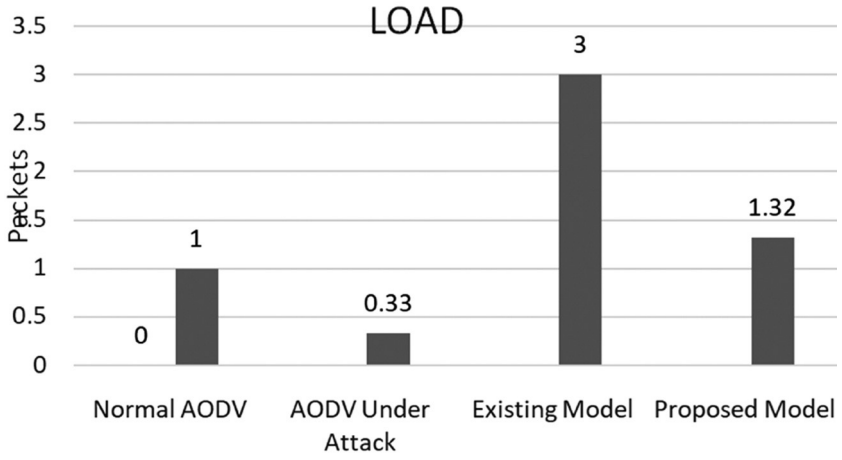
Figure 6 (a) shows the packet delivery ratio between the two models. The packet delivery ratio of the proposed model is 80%, the existing model has a 40% packet delivery ratio during attack, while the normal AODV has 90%, but the performance under attack dwindling to 20% under attack. Thus, the proposed model performed better than the existing model in terms of packet delivery ratio. The performance of the two models was also compared based on the load incurred during attack as depicted in Figure 6 (b). It is shown that the normal AODV incurred a delay of 5 ms when under attack; the delay experienced in existing model was 0.55 ms, which is far lower than the delay experienced in the normal AODV under attack. The performance of the existing model using the delay as metric seems inconsistent with the available data in the literature. The security measure embedded in the AODV protocol is a code which will take some time to run and thus should incur more delay than the normal AODV. This indicates that normal route maintenance packets are suspended in the existing model thus making the parameter result of the metrics unreliable. The last metric used for performance comparison is the load experienced in



(a) Packet delivery ratio of the proposed and the existing models.



(b) The delay experienced in the proposed and the existing models.



(c) The load experienced in the proposed and the existing models.

Figure 6.

the models. The load of the proposed model is 1.32 packets, while that of the existing model is 3.0 packets, as shown in Figure 6 (c). The proposed model performs better than the existing model.

7. Conclusion

In this paper, a prey-predator scenario is modeled and simulated in a stochastically dynamic environment. The AODV routing protocol, which is widely accepted as the "defacto" routing protocol for MANET, is used as the test bed for the simulation. Black hole, grey hole and DDoS attacks were used as the attacks' models on MANET. During the simulation period, the network environment is assumed to be hostile, with the attackers being persistent. The simulation results show that the security mechanism embedded in OADV did not add too much load on the routing protocol, therefore, the throughput of the system is still within an acceptable threshold. This work can be extended for other network attacks on the MANET. The work can further be fully implemented using an appropriate programming language.

Acknowledgment

The authors acknowledge TETFUND for the grant provided for this research through year 2020 research grant intervention (TETF / ES / DR&D-CE / NRF2020 / CC / 27 / VOL.1.) and ACE OAK-PARK, Obafemi Awolowo University, for providing the space for CySe LAB, where this research was conducted.

References

[1] A. M. Shantaf *et al.*, "Performance Evaluation of Three Mobile Ad-hoc Network Routing Protocols in Different Environments," in *Proc. of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2020, pp. 1–6. http://dx.doi.org/10.1109/HORA49412.2020.9152845

[2] P. Levis *et al.*, Overview of Existing Routing Protocols for Low Power and Lossy Networks. *Internet-Draft Draft-Ietf-Roll-Protocols-Survey-07, Internet Engineering Task Force*, 2009, (Work in progress).

[3] F. Abdel-Fattah *et al.*, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," in *Proc. of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019, pp. 28–33. http://dx.doi.org/10.1109/JEEIT.2019.8717449

[4] M. Karthigha *et al.*, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad Hoc Networks", in *Proc. of the 2020 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2020, pp. 396–402. http://dx.doi.org/10.1109/ICICT48043.2020.9112588

[5] C. Lin, "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation (SWANS)", 2006. Available: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.5477&rep=rep1&type=pdf

[6] S. Thapar and S. K. Sharma, "Attacks and Security Issues of Mobile Ad Hoc Networks", in *Proc. of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM)*, Jaipur, India, 2019, pp. 26–28. http://dx.doi.org/10.2139/ssrn.3356214

[7] S. Banerjee and K. Majumder, "Wormhole Attack Mitigation in Manet: A Cluster Based Avoidance Technique", *International Journal of Computer Networks and Communications,* vol. 6, no. 1, pp. 45–60, 2014.

[8] M. N. Ahmed *et al.*, "A Survey of MANET Survivability Routing Techniques", *International Journal of Communications, Network and System Sciences* vol. 6, no. 4, pp. 176–185, 2013.

[9] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & PreventionApproaches for Network Layer Attacks", *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[10] M. F. Elettreby, "Two-prey One-predator Model, Chaos, Solitons and Fractals", vol. 39, no. 5, pp. 2018–2027, 2009. http://dx.doi.org/10.1016/j.chaos.2007.06.058

[11] R. J. Ellison *et al.*, "Survivability Assurance for System of Systems", Technical Report Number: CMU/SEI-2008-TR-008 submitted to Software Engineering Institute at Carnegie Mellon University http://dx.doi.org/10.1184/R1/6584486.v1

[12] Y. Zhou *et al.*, "Research on Survivability of Mobile Ad-hoc Network", *Journal of Software Engineering and Applications*, vol. 2, no. 1, pp. 50–54, 2009. http://dx.doi.org/10.4236/jsea.2009.21008

[13] H. Zhao and P. Ratazzi, "Providing Physical Layer Security for IoTs in the Last Mile", *Journal of Computing and Information Technology*, vol. 29, no. 2, pp. 89–111, 2021. http://dx.doi.org/10.20532/cit.2021.1005317

[14] F. Dressler and O. Akan, "Bio-inspired Networking: from Theory to Practice", *IEEE Communications Magazine*, vol. 48, no. 11, pp. 176–183, 2010.

[15] C. Pankaj and C. Sachin, "Bio-Inspired Methods for Efficient MANET", *International Journal of Science and Research (IJSR)*, vol. 2, no. 5, pp. 37–40, 2013. https://www.ijsr.net/get_abstract.php?paper_id=IJSROFF2013213

[16] A. Idmbarek *et al.*, "Interrelationships between Prey and Predators and How Predators Choose Their Prey to Maximize Their Utility Functions", *Hindawi Journal of Applied Mathematics*, vol. 2021, Article ID 6619500. https://doi.org/10.1155/2021/6619500

[17] V. R. Verma *et al.*, "Performance Improvement in MANET Routing by Paradigm Shifting Through Mobile Agent Approach", in *Proc. of the International Conference on Advances in Electronics, Electrical and Computational Intelligence (ICAEEC)*, 2019. http://dx.doi.org/10.2139/ssrn.3574033

[18] P. Amish and V. Vaghela, "Parmar Amish and Vimalkumar B. Vaghela Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", *Procedia Computer Science*, vol. 79, pp. 700–707, 2016. http://dx.doi.org/10.5120/ijca2017915376

[19] H. Ghayvat *et al.*, "Advanced AODV Approach for Efficient Detection and Mitigation of Wormhole Attack in MANET", in *Proc. of the 2016 10th International Conference on Sensing Technology (ICST)*, 2016, pp. 1–6. http://dx.doi.org/10.1109/ICSensT.2016.7796286

[20] R. Arun Prakash *et al.*, "Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad hoc Network by Coordinator", *Applied Mathematics & Information Sciences*, vol. 12, no. 1, pp. 233–237, 2018.

[21] M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," *IEEE Access*, vol. 9, pp. 11872–11883, 2021. http://dx.doi.org/10.1109/ACCESS.2021.3051491

[22] S. S. Joshi and S. R. Biradar, "Communication Framework for Jointly Addressing Issues of Routing Overhead and Energy Drainage in MANET", *Procedia Computer Science*, vol. 89, pp. 57–63, 2016.

[23] C. Ran *et al.*, "An Improved Routing Security Algorithm based on Blockchain Technology in Ad Hoc Network", *Journal of Wireless Communication Network*, 2021. http://dx.doi.org/10.1186/s13638-021-01938-y

[24] P. Bondada *et al.*, "Data Security-Based Routing in MANETs Using Key Management Mechanism", *Applied Sciences*, vol. 12, 2022. http://dx.doi.org/10.3390/app12031041

[25] S. J. Sultanuddin and M. Ali Hussain, "Intrusion Detection in MANET through Machine Learning Approach", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 11, no. 3. http://dx.doi.org/10.35940/ijitee.C9679.0111322

[26] D. Tesfay *et al.*, "An Intrusion Prevention System embedded AODV to protect Mobile Adhoc Network against Sybil Attack", in *Proc. of the International Conference on Data Science, Machine Learning and Artificial Intelligence, DSMLAI '21'*, pp. 57–64. http://dx.doi.org/10.1145/3484824.3484915

[27] A. Sohail *et al.*, "Survivability Analysis of MANET Routing Protocols under DOS Attacks", *Ksii Transactions on Internet and Information Systems*, vol. 14, no. 9, pp. 3639–3661, 2020. http://dx.doi.org/10.3837/tiis.2020.09.004

[28] M. I. Talukdar *et al.*, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature", *Hindawi Wireless Communications and Mobile Computing*, vol. 2021, no. 13. http://dx.doi.org/10.1155/2021/6693316

[29] A. J. Lotka and E. W. Kopf, "Elements of Physical Biology", *Nature*, vol. 116, 1925. http://dx.doi.org/10.1038/116461b0

[30] V. Volterra, "Lessons on the Mathematical Theory of Struggle for Life" (Original: "Leçons sur la théorie mathématique de la Lutte pour la vie"). Paris: Gauthier-Villars, 1931.

[31] A. W. Bateman *et al.*, "When to Defend: Antipredator Defenses and the Predation Sequence", *The American Naturalist*, vol. 183, no. 6, 2014.

Received: August 2022
Revised: April 2023
Accepted: May 2023

Contact addresses:
Abiodun Akinwale
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: logistronics@yahoo.com

Emmanuel Ajayi Olajubu
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: emmolajubu@oauife.edu.ng

Ganiyu Adesola Aderounmu
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: gaderun@oauife.edu.ng

Abiodun Akinwale is the CEO/MD of Logitronic Systems Ltd. He holds a BSc degree in computer engineering from Obafemi Awolowo University, Ile-Ife, Nigeria. He also holds MSc and PhD degrees from the same University. He is an experienced digital communications professional with over 28 years' experience. As an industry-based researcher, he is interested in bridging the gap between industrial ICT practice and necessary theoretical foundations of the academic to build real-world applications. He is a researcher in the Cyber Security (CySe) Lab at the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile Ife, Nigeria. His current effort aims at developing integrated multilayered cyber-defense software for IT/OT applications. He has a number of publications in reputable journals. He is adept in designing suitable algorithms and models for cyber security solutions for mission critical systems.

Emmanuel Ajayi Olajubu holds MSc and PhD degrees in computer science from the Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria. He is currently a professor, coordinating cyber security research group activities at CySe LAB, ACE Building Complex, Incubation Centre, Obafemi Awolowo University. He is a member of the Nigerian Computer Society (NCS), Computer Professional Registration Council of Nigeria (CPN), and International Association of Engineers (IAENG). He has many published articles in reputable journals and referred conference proceedings. His research interests are in the area of distributed systems, cyber-physical systems, and cyber security, including network security. He was a former acting head at the Department of Computer Science & Engineering, Obafemi Awolowo University.

Ganiyu Adesola Aderounmu is a professor of computer science and engineering from the Obafemi Awolowo University, Ile-Ife, Nigeria. He is a full member of the Nigeria Society of Engineers (NSE) and a registered computer engineer with the Council for Regulation of Engineering Practice in Nigeria (COREN). He is also a full member of the Nigeria Computer Society (NCS) and Computer Professional Registration Council of Nigeria (CPN). He has over 30 years of experience in teaching and research. He is an author of many journal articles in Nigeria and abroad. His research interests include computer communication and network and cyber security. He is a visiting research fellow to the University of Zululand, Republic of South Africa. He was the former head of the Department of computer Science & Engineering, former dean at the Faculty of Technology, former president of the Nigeria Computer Society (NCS), and the former director of Information Technology and Communication Unit (INTECU). He is the center leader and director of the Africa Centre of Excellence (ACE): OAU ICT-Driven Knowledge Park, Obafemi Awolowo University, Ile-Ife, Nigeria.