Emmanuel A. Olajubu
Abiodun Akinwale
Kazeem Ibraheem Ogundoyin

AN OCTOPUS-INSPIRED INTRUSION DETERRENCE MODEL IN DISTRIBUTED COMPUTING SYSTEM

Abstract *The study formulated and evaluated a model for effective management of malicious nodes in mobile Ad-hoc network based on Ad-Hoc on- demand distance vector routing protocol. A collaborative injection model called Collaborative Injection Deterrence Model (CIDM) was formulated using stochastic theory. The definition of the model was presented using graph theory. CIDM was simulated using three different scenarios. The three scenarios were then compared using packets delivery ratio (PDR), routing load, throughput and delay as performance metrics. The simulation result showed that CIDM reduce considerably the rate of packets dropped caused by malicious nodes in MANET network. CIDM did not introduce additional load to the network and yet with produce higher throughput. Lastly, the access delay with CIDM is minimal compared with convectional OADV. The study developed a model to mete out a punitive measure to rogue nodes as a form of intrusion deterrence without degrading the overall performance of the network. The well known CRAWDAD dataset was used in the simulation.*

Keywords CIDM; MANET; Intrusion detection; Mobility; Routing Load; Throughput; 1-hop neighbors; wireless; Malicious; Injection

Citation Computer Science 17 (4) 2016: 483–502

1. Introduction

Mobile Ad-hoc Network (MANET) is an example of distributed network which comprises of mobile nodes with no central coordinating unit, generally dynamic and heterogeneous in nature, and all the nodes are battery powered [22]. Collaboration is the main thrust of MANET. This form of network is very spontaneous and self-organizing; and this has proved very useful in emergency situation especially in military warfare. Nevertheless, the distributed, dynamic and infrastructure less nature of MANETs makes it very vulnerable to network attacks. One active network attack is Black hold attack, this attack result in network traffic distortion. The attacks in this category are denial of service (DoS) attack [11, 26], network packet editing (modification, replication and deletion of exchange data), traffic distortion, IP spoofing [11, 30]. The aim of these attacks mostly is to dwindle network communication performance of the network by attacking neighbouring nodes [20, 21, 24]. It was reported in [2] that incessant recurring attacks by blocked malicious nodes having their full power and computing resources intact have been one of the main problems militating against widespread deployment of MANETs. Despite the presence of Intrusion Detection Systems in ad-hoc networks, malicious nodes have been able to spoof their IP and MAC addresses and re-launch attacks after being blocked. It is therefore very necessary to develop a strong deterrence system that will not only block malicious systems, but goes a step further to proper effective management of such node(s) by running down the resources of the node(s) through the collaborative injection from the one hop neighbours. To the best of our knowledge, this is the first work that would to decisively manage a malicious node by meting some punitive measures to any offending nodes in the network.

The paper presents a model that manages a malicious node by flooding the offending node with replicated deluge packets by one-hop neighbor nodes to run down the resources of the malicious node. Thus, the system is referred to as collaborative intrusion deterrence model (CIDM). It serves as deterrence against future misbehavior of any node in the network. This new security model – based on CIDM – is thus proposed for MANETs (which is applicable to other distributed systems with a little or no modification) was inspired by the natural defensive mechanism of the biological Octopus. Most octopus species are equipped with an ink sac that spews out a stream of dark liquid called cephalopod ink into the water when the creature is threatened. When frightened, an octopus often swallows water with its body and ejects it forcefully. This not only propels the animal away from the danger, but also forces out a trail of ink. This ink, which may be red, brown, or black, is made of melanin, which visually distracts, confuses, and perhaps even frightens the predator. Secondly, it paralysis the predators sense of smell or sight so that it cannot apprehend the creature and lastly, the ink clouds the water to help give the octopus time to escape. The technique employed here is the first time data flooding packet replication was used to enhance security in ad hoc networks [4, 32]. The next section highlights some relevant works on intrusion detection systems; section three presents our model design while section four discusses our experimental design in OPNET environment. The following section describes our simulation results while section six concludes the paper.

2. Related Works

The exponential growth and deployment of MANETs has made security issues in the network an attracted some attentions in the research arena. Many researchers have attempted to propose solutions to security mechanisms in MANETs. Shakshuki *et al.* reported in [28] that their proposed model called Enhanced Adaptive Acknowledgment (EAACK) requires both the sender and receiver to digitally signed and verified all packets during communication. The proposed model implemented DSA and RSA form of digital signature. It was demonstrated that the model has the capacity to detect quite range of attacks within MANET but this increases the network load of the network with narrow bandwidth. Also, the scheme did not propose any punishment for such malicious node on MANET. Lui *et al.* in [19] developed a scheme which can query each data packets sent over three consecutive nodes through the source node to the destination node. The destination and every node on the path will be required to send back acknowledgment to the source node. The arrival of TWOACK packet indicates successful delivery of the packet from node say A to node say C via some intermediate B. For instance, the arrival of the TWOACK is within a specified time, any arrival outside the specified time is termed arrival failure, which define nodes A and B as malicious nodes. The generation of TWOACK after some time threshold,started to add extra load on the network, also this scheme do not apportion any penalty to the malicious node.

Game theory applications have been explored to find lasting solution to MANET security breaches. A game theory model was formulated by [15]. In the model, the researchers presented the scheme as a two person zero-sum game. The service provider which is the first player tries to maximize the detection of malicious node by increasing its probability while the attacker minimizes the probability of been detected by network IDS. The challenge with the work is that, it is assumed that both player in the game have full information about the network which is not so in real network. Even when the attacker is detected no punishment is stipulated for its offense on the network. Another game theory solution for MANET that models the cooperation and selfishness of the networks are discussed in [1, 7, 18]. The schemes provide methods for each node on the network to decide either to transmit packet or not transmit a packet based on the trade-offs involved. The energy consumption and network throughput concepts involved in collaborating with other nodes in this model ensures cooperation. This cooperation scheme ensures that a selfish node that does not obey the network rules receives a low throughput. Like any other game theory based solutions, this model assumes the complete information of the game, which implies all nodes are fully aware of network metrics and structure. Farrahi and Ahmadzadeh in [8] modeled an IDS Nave Bayes, with support vector machine and OneR algorithms. The model achieved better detection accuracy for DoS attacks but also rise high false alarm rate for U2R and R2Lattacks. In the work of Subba *et al.* presented in [30] modeled a Bayesian game based model for detecting back hole attacks such as DoS and traffic distortion in MANET. The model uses active Lightweight IDS to calculate the rate of packet forwarding of node n_i . If the packet forwarding rate is less than a defined threshold, the probability of been malicious the node is updated using Bayes rule. The history profile of node n_i is also updated using Bayes rules. The system models the interaction between defender and node n_i as a non cooperative game. The model is well articulated and the result is profound, but the model did not recommend and penalty for the offending node.

Senthilnayaki *et al.* in [27] developed an a model based on gain ratio as feature selection technique. Two methods of classification techniques used was called support vector and rule based machines. These were used to identify the class label in the system. The model developed provided a higher degree of accuracy for detecting DoS but have no penalty for the malicious node. Saxena and Richariya in [25] devised a model that resulted in developing an intrusion detection model based on feature selection and SVM which was integrated with particle swarm optimization. The analysis of the model was profound, but the overhead of computing the employed SVM and particle swarm optimization was neglected which is quite crucial to the performance of the model. The model also failed to take decision on the offending node. Likewise a model was developed in [31] which used the technique of chi-square feature selection and multi class support vector machine (SVM). The logic of the model is to develop a multi-class SVM that decrease the training and testing time which can increase the detection accuracy of malicious nodes on the network. Balajinath and Raghavan in [3] employed genetic algorithm to learn users behavior pattern, the future usage of the users can be predicted from the past history of the users. Any form of deviation from users pattern is seen as intrusion detection. The users behavior is described in this work using a 3-tuple: Match index, Newness index and Entropy index. The system used the values of the 3-tuple as a command sample in the user session and then compare it with non-intrusion behavior. In wireless environment, multi-agent systems was developed in [23, 29] and [6] as a novel way of solving intrusion on challenges especially in MANET environment. Other models used to address the challenge are swarm intelligence [16] even the audit principle have been applied by Wang *et al.* in [33] where the volume of data to be processed is massive for intrusion detection purpose. Grey-theory also has been attempted as panacea for this challenge. Qin *et al.* in their work reported in [5] proposed the grey theory which was claimed to have some advantages and superiority on earlier used schemes because of its ability to cope with large data. The scheme has no penalty for intruding nodes.

There are existing models that used the concept of information deterrence such [9, 13, 14] and [12]. All the models are not relevant and cannot be applied to security in MANETs environment. Therefore, so far in literature, we are yet to find a model developed to serve as a deterrence system which can apportion penalty measure to malicious node on any MANETs. The propose model is seated under an existing

IDS, and offers some measure of punishment to the erring node by flooding such node with packets from one-hop neighbors so that the computing resources of the node especially the battery are completely depleted and removed from the network.

3. Model Design

The proposed CIDM focuses on effective method of managing malicious nodes in MANET. This implies that the new model adds a new module to existing IDS system models. In designing the CIDM model, the following issues were resolved:

i. The CIDM model is network-based because of the collaboration of neighbor nodes in the injection process.
ii. Only one-hop neighbors of the malicious node are involved in the process so that the entire network is not flooded by bombarding packets.
iii. The injection process has a threshold value after which the injection stops and the collaborating nodes can do other internal processing or routing work.

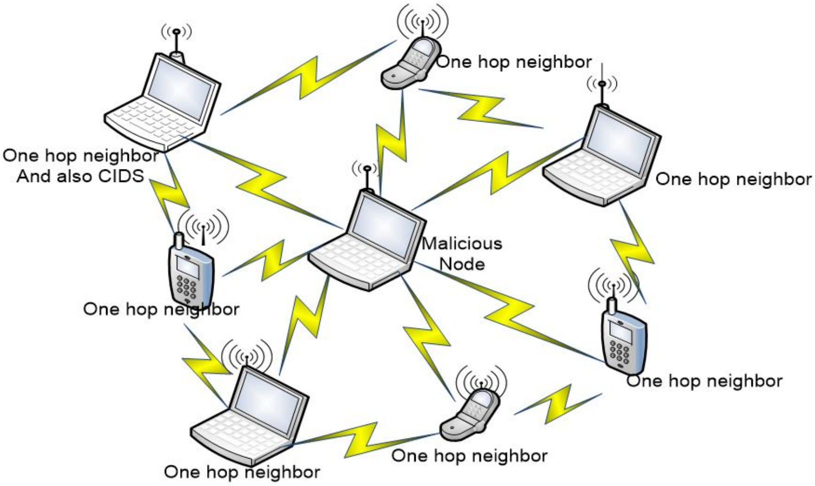


Figure 1. The CIDS Conceptual Model.

Our model design depicted in Figure 1 represents a simple MANET environment, where there is one malicious node at the center of the network.

The conceptual model shows one-hop neighbors around the malicious node which are triggered by the CIDM neighbor to flood the malicious node with packets so as to rundown the computing resources (battery power) of the offending node. The model predisposes that all one-hop neighbors of a node are well connected and therefore serve as a communication link to other nodes on the network. The aim of this model is to prevent the malicious node from immediately going to spoof its IP and MAC addresses and re-launch attacks after being blocked. Once, the battery is rundown, the malicious node lacks wherewithal to re-launch another attack. In designing this conceptual model, we assume that an effective intrusion detection system that can mitigate any act that breaches network security exists as a facility on the network for security purpose. Thus, the CIDM sits at the top of this existing IDS system in the network to further render an effective management policy that will make it difficult for offending node(s) to re-launch any attack on the network.

The CIDM starts the process by initiating a counter that keeps track of nodes in the network. The model then calls on the neighbor discovery facility in AODV to discover the one-hop neighbors of any new node joining the network. In this way, the CIDM node acts as the cluster head. Next it initiates the intrusion detection systems and scans each node for malicious activity. If a node had already been scanned, it transfer control to the next node and repeats the process. Once a malicious activity has been detected, the CIDM launches its response model by first, collecting the parameters of the offending node from the IDS system, then checks its routing table for one-hop neighbors of the node. It then sends an injection command to all the one-hop neighbor-nodes instructing them to send packets to the malicious node for a time frame. The inject command includes the amount of packets to inject and the length of time necessary to achieve the bombardment after which the process starts all over. This period of collaborative injection i.e. the amount of packets to be injected by the 1-hop neighbors is determined by number of 1-hop neighbors surrounding the malicious node and also by the present value of the battery power of the malicious node. Figure 2 presents the algorithm in form of flowchart. It is interesting to know that there will not be much increase in the routing protocol overhead of the CIDM despite the collaborative injection, since the injection is carried out only by one-hop neighbors of the malicious node. The operation of CIDM is to augment conventional IDS, thus present a formal definition of MANET using graph theory. Also, CIDM model was formulated using stochastic theory which is presented in the following section.

3.1. MANET Formal Definition Using Graph Theory

In developing an algorithm for CIDM, a model that deters malicious nodes from re-attempting attacks on a MANET network system, there is the need to capture the essential characteristics of a MANET. A MANET was formally described using Graph representation as: Let M be a MANET with state space S, the elements of M are mobile devices V according to Larson and Hedman [17]. Each mobile node in V is a pobabilistic finite state machine. A MANET is a random process defined as a graph (G_t) and a space (S_t) at time t, that is,

$$M = (G_t,\ S_t) \tag{1}$$

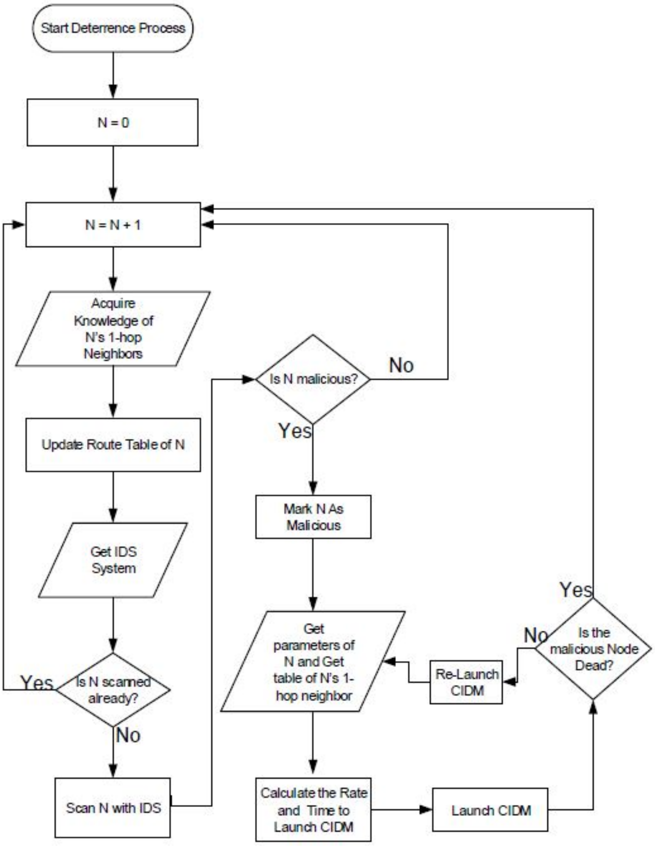


Figure 2. CIDM Algorithm.

Where a graph is defined as a set of mobile nodes (V) and edges/links (E) that is,

$$G_t = (V,\ E) \tag{2}$$

$$V = V_1, V_2, V_3, \ldots, V_N \tag{3}$$

$$E = (V_x,\ V_y) : V_x \neq V_y \& (V_x \bigwedge V_y) \in V \tag{4}$$

$$S_N = V_i,\ V_i \tag{5}$$

$$L_i = (x_i,\ y_i,\ z_i) \tag{6}$$

Where x, y and z are the space coordinates of location L at any particular time. From Equation (1), G_N is a graph with mobile node set V and a set of link (edges) E_N. S_N is the set of mobile node V at location L, subject to Markov, mobility and medium constraints which is presented in the following section.

3.1.1. The Markov Chain Mobility constraints

Let P_t, Q_t, be the current state of the MANET network, then the next state of the network will then be P_{t+1}, Q_{t+1} which is not dependent on the preceding states (P_1, Q_1), $\ldots(P_{t-1}$, $Q_{t-1})$, this is referred to as Markov chains. The transitional mobility probabilities will then be P_r $[(P_{t+1},\ Q_{t+1}) \mid (P_t,\ Q_t)]$ are independent of t. The transitional probabilities will then generate the mobility distribution of this network. μ is definitely determined by the internal states of the nodes of P and nature. The mobility variables are defined as follows:

i. dist$(N_p,\ N_q)$ t is the distance between nodes x and y at time t
ii. n is the number of nodes and i is the index and $i = 1,\ 2,\ \ldots,\ n$
iii. $A_p(t)$ is the average distance for node p to all other nodes at time t
iv. M_p is the average mobility for node p
v. T is the simulation time and Δt is the simulation step
vi. M_b is the mobility for entire MANET

$$A_p t = \frac{\sum_{t=1}^{n} dist(n_x n_i)}{n-1} \tag{7}$$

$$\frac{\sum_{t=0}^{T} \mid (A_t - A_x(t+\Delta t)) \mid}{T - \Delta t} \tag{8}$$

$$M_b = \frac{\sum_{t=1}^{n} M_i}{n} \tag{9}$$

3.1.2. The Markov constraints Communication medium constraints

In a MANET environment, the following communication medium constraints hold:

i. If p transmits a packet at time t, this is received simultaneously at time $t' > t$ by its neighbors, then the source node is promiscuous.
ii. Bidirectional: If p and q are neighbors, then q will receive any message transmitted by p and p will likewise receive any message transmitted by q.
iii. a node p cannot be connected back to itself

From the foregoing, the data structure of the communication between the nodes can be captured by an $n \times m$ matrix as shown in equation (10) below for a MANET with 10 nodes.

$$P = \begin{array}{c|cccccccccc} & A & B & C & D & E & F & G & H & I & J \\ \hline A & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ B & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ C & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ D & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ E & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ F & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ G & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ H & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ I & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ J & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array} \tag{10}$$

Matrix 1: Incidence Matrix of Graph G with 10 nodes

3.2. Simulation Data Preparation

The standard dataset used for the simulation of the Collaborative Intrusion Deterrence Model (CIDM) was obtained from the CRAWDAD (A Community Resource for Archiving Wireless Data at Dartmouth) dataset [10] from Dartmouth University. This dataset was collected from the outdoor runs of MANET based on the AODV algorithm. The outdoor experiment for the dataset took place on an athletic field measuring 225 meters by 365 meters far off from the campus center to prevent interference from hotspots. The routing experiments ran on top of 41 laptops. Forty laptops ran the protocol and one was used as the control system. The wireless radio of each laptop was set to transmit at 2 Mbps. Finally, each laptop had a GPS unit attached to the serial port to locate the 3−dimensional coordinates of each node. The traffic for the network was generated by special traffic generators installed on each node. These generators send streams of packets to randomly selected nodes in the network. Users moved continuously throughout the experiment.

3.2.1. Dataset format

There are four types of line entries:

i. TIN [size] [seconds portion of timestamp] [usecs portion of time stamp] [src] [dest] [seq #]

ii. SIN [size] [seconds portion of timestamp] [usecs portion of time stamp] [src] [dest] [previous hop ip] [seq #]

iii. TOUT [size] [seconds portion of timestamp] [usecs portion of time stamp] [src] [dest] [seq #]

iv. SOUT [size] [seconds portion of timestamp] [usecs portion of time stamp] [src] [dest] [previous hop ip] [seq #]

The TIN (In from Tunnel) entries describe a packet that was generated by this node's traffic generation process and that is being passed down to the routing layer to be sent out on its way. The TOUT (Out over Tunnel) entries describe a packed generated by a traffic generation process arriving safely at its destination. The SIN (In from Socket) and SOUT (Out over Socket) entries describe the transmission and receipt of a traffic generation packet, respectively, at a hop-by-hop level Table 1. In other words, if a packet is generated by the traffic gen program at node 1 bound for node 3, and to get there it bounces first from 1 to 2 then 2 and subsequently to 3, then a TIN for this packet will appear at 1, a TOUT at 3, and a SOUT at 1, SIN at 2, SOUT at 2, and SIN at 3.

Table 1

CRAWDAD sample data generated from node1 (Source: [19]).

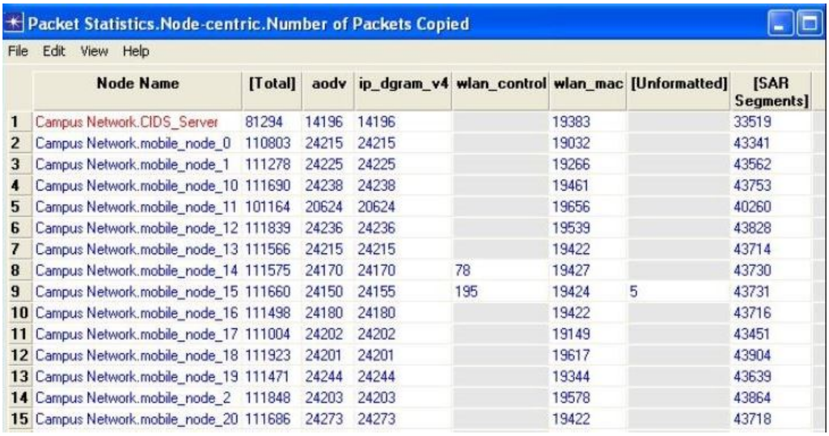
Process	Size	Time (sec)	Source Address	Destination Address	No
TOUT	1110	1066402501	158907	11.0.0.1	11.0.0.3
TIN	1110	1066402501	302979	11.0.0.28	11.0.0.1
TIN	1110	1066402501	314045	11.0.0.3	11.0.0.1
TIN	1110	1066402501	392057	11.0.0.26	11.0.0.1
TIN	1110	1066402501	457447	11.0.0.18	11.0.0.1
TIN	1110	1066402502	450568	11.0.0.48	11.0.0.1
TIN	1110	1066402502	502602	11.0.0.40	11.0.0.1
TOUT	1110	1066402513	188667	11.0.0.1	11.0.0.3
TIN	1110	1066402513	329668	11.0.0.3	11.0.0.1

3.2.2. Packet statistics

The results of packets generated and used to inject malicious node are shown in Figure 3. The injection to one black hole node was done with the consideration of the available battery power to the malicious node and also with number of 1-hop neighbor surrounding the malicious. This process generated a 5-second packet injection to malicious node so that the network is not congested with packets. The packet injected was generated within the network using data from CRAWDAD dataset as the prototype data guide.

4. Experimental Design of AODV routing protocol in OPNET

The experiment for the work was setup using the wizard, which was a campus network with an area of dimensions 1 km × 1 km was designed with 40 mobile nodes and a server was deployed. The mobile nodes and the server were spread randomly within the geographical area. In this scenario, the mobile nodes received traffic from a common source. The Ad Hoc routing protocol was set to AODV and UDP traffic used to study the effects of the protocol. This will enable an evaluation of the performance of the protocol in UDP based applications such as web and file transfer. In the profile configuration, an SNMP application was deployed for our study. All other settings were left at the default: the nodes were WLAN mobile clients with a data



	Node Name	[Total]	aodv	ip_dgram_v4	wlan_control	wlan_mac	[Unformatted]	[SAR Segments]
1	Campus Network.CIDS_Server	81294	14196	14196		19383		33519
2	Campus Network.mobile_node_0	110803	24215	24215		19032		43341
3	Campus Network.mobile_node_1	111278	24225	24225		19266		43562
4	Campus Network.mobile_node_10	111690	24238	24238		19461		43753
5	Campus Network.mobile_node_11	101164	20624	20624		19656		40260
6	Campus Network.mobile_node_12	111839	24236	24236		19539		43828
7	Campus Network.mobile_node_13	111566	24215	24215		19422		43714
8	Campus Network.mobile_node_14	111575	24170	24170	78	19427		43730
9	Campus Network.mobile_node_15	111660	24150	24155	195	19424	5	43731
10	Campus Network.mobile_node_16	111498	24180	24180		19422		43716
11	Campus Network.mobile_node_17	111004	24202	24202		19149		43451
12	Campus Network.mobile_node_18	111923	24201	24201		19617		43904
13	Campus Network.mobile_node_19	111471	24244	24244		19344		43639
14	Campus Network.mobile_node_2	111848	24203	24203		19578		43864
15	Campus Network.mobile_node_20	111686	24273	24273		19422		43718

Figure 3. Packet statistics showing injection to node 15.

rate set at 11 Mbps operating with a default power of 0.005 watts, the destination was a WLAN server also with a data rate of 11 Mbps and transmitting with 0.005 watts power. For mobility, random waypoint mobility model was used because it is a simple and widely accepted mobility model to depict more realistic mobility behaviour. The nodes move at a constant speed of 10 m/s. When the node reaches its destination, it pauses for 300 seconds and then chooses a new random destination. The experiment was simulated for 3600s. Table 2 shows the parameter settings for the first experiment, while Figure 4 shows the experiment design environment.

Table 2

Parameter settings for normal AODV protocol implementation.

Process	**Size**
Simulation Time (s)	3600
Number of nodes	40
Simulation Area (m)	1000 × 1000
Mobility Model	Default Random Waypoint
Pause Time (s)	300
Mode Speed (m/s)	10
Transmit Power (W)	0.005
Data Rate (Mb/s)	11
Packet Reception Power Threshold (dBm)	-95
Traffic	SMNP
Traffic Model	UDP
MAC protocol	IEEE 802.11b
Packet Size (bytes)	1200

To make a case of black hole attack, nodes 10 and 15 was randomly taken as malicious nodes on the network. The additional parameters and changes to configurations of the malicious nodes 10 and 15 which exhibit anomalous behaviour are given in Table 3. The buffer size was made very small for the node thus causing it to become a sink for packets.

Table 3

Additional Parameters setting for Black hole.

Parameter	Value
Has Function	SHA-1
Source Node	1024
Packet Inter Arrival	Uniform (1, 11)
Buffer Size (bytes)	1024

The design of the AODV MANET in OPNET was directly modified to become a function within our collaborative injection deterrence model. Additional parameter settings for the case of CIDM is shown presented in Table 4 while Figure 6 presents the case scenario. After running the simulation, we observed the response of CIDM on the malicious node 15 by gathering its object statistics. Node 14 was chosen as the one-hop neighbour and its destination addressed pointed to node 15, which is the malicious node. The destination address of node 15 was set to zero so that it is effectively blocked from the network. The injection time was limited to just 5 seconds so that the entire network does not become congested.

Table 4

Additional Parameters setting for Implementing CIDM.

Parameter	Value
Node 15 IP Address	192.0.1.17
Node 15 Destination Address	0.0.0.0
Node 10 destination Address	192.0.1.17
Buffer Size (bytes)	256000
Injection Time (s)	5

5. Simulation Results Discussion

In this section, the simulation results for the performance metrics are: Delay, Routing load, Network throughput and Packet drop rate. Global statistics for the entire network was collected as well as object statistics for node 15 and present time-average values were shown. The scenarios are: (i) normal AODV deployment without any malicious activity, (ii) AODV with two black hole attacks and (iii) CIDM response to the malicious activity. Further, the statistics showing the packet injected to the malicious node 15 by neighbor node 4 is shown.

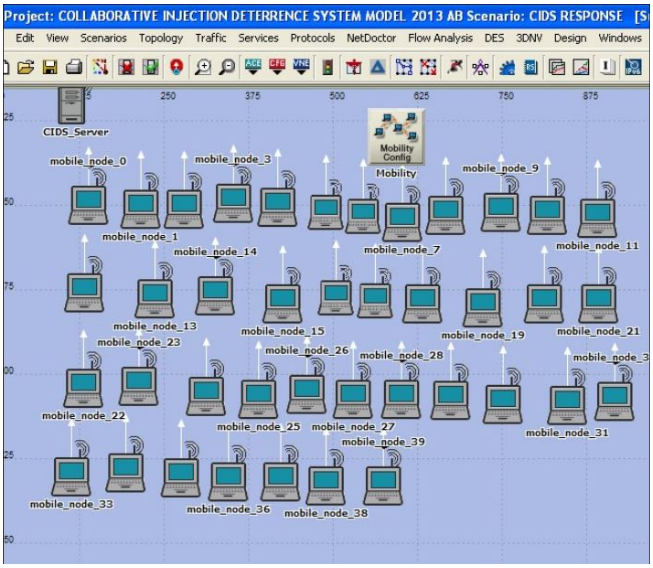


Figure 4. CIDM simulation Experiment Environment.

5.1. Delay

Comparative analysis of the three scenarios presents interesting results as shown in Figure 5. In all scenarios considered, it was observed that for Media Access, CIDM has the lowest delay which means that routes in the network are always ready whenever the MAC layer has traffic to transmit. Periodic routing updates keep fresh routes available for use. The absence of high latency induced by the route discovery processes in CIDM explains its relatively low delay. However for end-to-end delay, the performance CIDM is lower than that of normal AODV. This is because of the injection period. This implies that if a node is performing the injection process, any packet meant for that destination will have some delays. This implies that the CIDM injection time must be kept very low for optimum performance of the network. However, from the result, CIDM introduction drastically reduced the end-to-end delay caused by black hole attacks.

The MAC access delay in the network with two black hole attacks was a bit lower than normal AODV routing protocol. This is consistent with the fact that a black hole node advertises itself as having the shortest path to a node it wants to intercepts. Thus network traffic is diverted to the malicious node without delay. On introduction of our CIDM response, the black hole was completely removed from the network and thereafter injected with meaningless packets to run down the resources of the node. The blocking of the node removes all diverted traffics thus leading to considerably less end-to-end delay in the network.

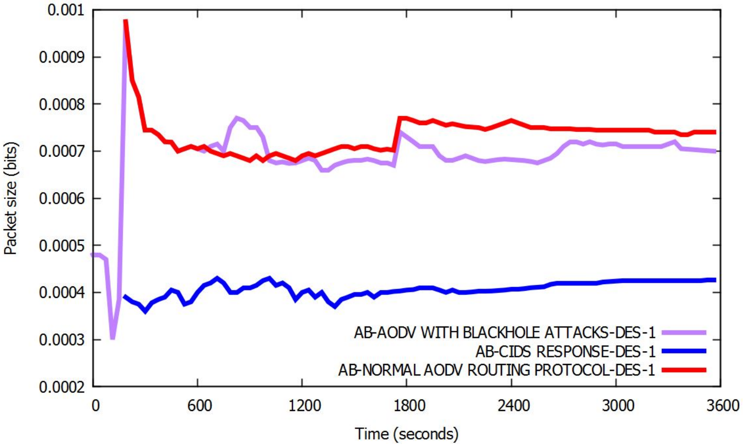


Figure 5. Media Access Delay.

5.2. Routing load

For the routing load analysis, it was observed that black hole sent the highest amount of routing traffic into the network followed by the CIDM. Following CIDM is normal AODV with the least amount of routing traffic sent. This observation is valid because of the route packets introduced by the black hole attack which sends reckless packets into the network. Therefore, in terms of routing overhead, CIDM performed comparatively at the same level with normal AODV. The superiority of CIDM comes from the advantage of its routing operation, since CIDM sends routing traffic into the network only when there is intrusion in the network thus eliminating the overhead due to unnecessary routing traffic. All intermediate nodes that are not one-hop neighbors use cached information to relay traffic and do not send replies during injection commands. Only one-hop neighbors respond to the CIDM command by sending injection to the malicious nodes in the network. In summary, network routing load results shows the effect of black hole attack on the MANET network. The load is much higher because of fake RREQ and RREP messages in the network. This implies that route maintenance messages increased with black hole attack. As shown in Figure 6, our CIDM algorithm introduced a fairly acceptable amount of route load. The reason for this is that our model injected packets to malicious nodes by only one-hop neighbors of the offending node thus reducing route load. Also, the time for the injection of packets was limited to just 5 seconds so as not to flood the entire network with CIDM packets. Within the limits of our threshold injection time, it can be stated that it is safe to deploy CIDM to MANETs as it did not introduce unnecessary packets into a network.

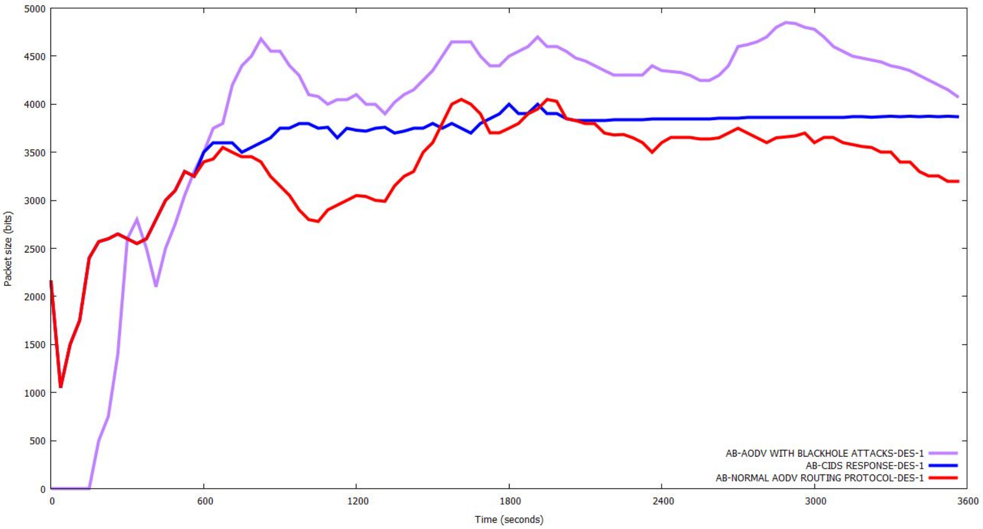


Figure 6. Routing load result.

5.3. Network throughput

Network throughput is defined as the amount of data that can be successfully delivered from source node to the destination node. The throughput of CIDM was lower than AODV throughput when the system was under attack by a malicious node as depicted in Figure 7. This is due to network resources deployed to counter the intrusion to the network. It must be stated that in evaluating this metric, adequate security is not cheap to implement. More often than not, security for any system will take additional resources for normal operation. Thus, resource usage is a trade-off for implementing security. In military-tactical formations where security is of the highest essence because of nearby enemies, reducing the throughput to combat the enemy for some time makes sense. However, more research will be made in future work to see how improvement can be made on this metric. Since throughput is the ratio of the total amount of data that a receiver receives from the sender to the time it takes for the receiver to get the last packet, a low delay in the network should translate into higher throughput. We expected higher throughput for CIDM.

5.4. Packet delivery

Simulation result shows a very high rate of dropped packets when the network was attacked by two black hole nodes. The two nodes act as a sink, dropping all packets after diverting traffics to them. When CIDM was launched, it effectively blocked and withdrew all computing resources of the two black holes nodes. Thus, the rate at which packets are dropped on the network drastically reduced to the minimum. Figure 8 showed the result of dropped packets without and with CIDM system at the

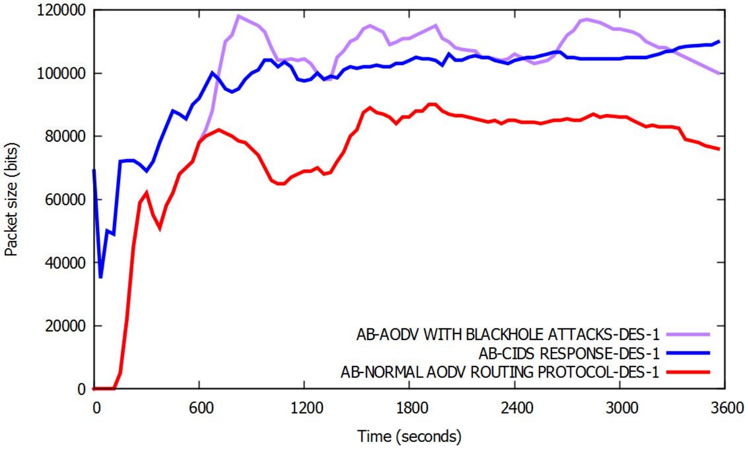


Figure 7. Network throughput result.

speed of 10 m/s. The number of packets dropped without the CIDM was very high but when CIDM was launched, it reduced the rate of packet dropped. We observed low packet delivery for AODV and CIDM in the scenarios considered.

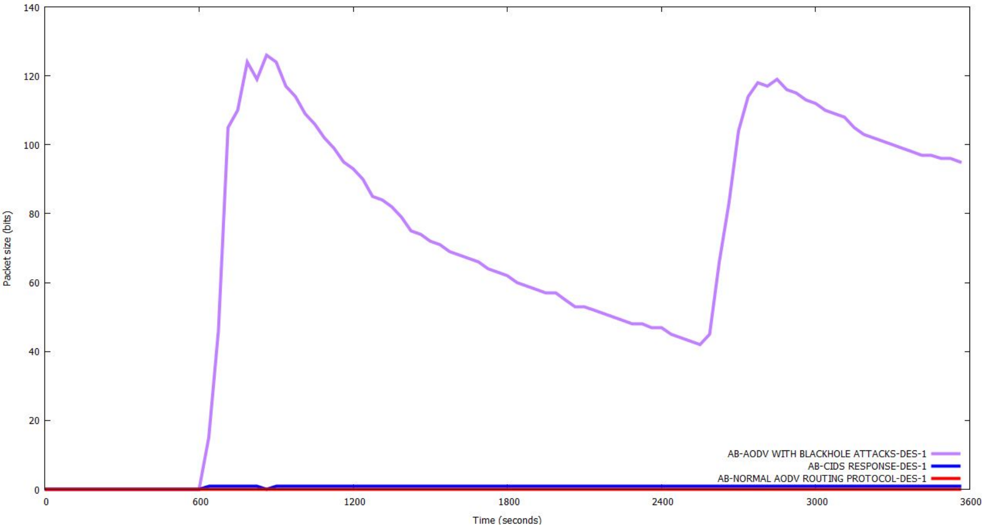


Figure 8. Rate of dropped packets.

6. Conclusion

A cyber security model that meted some decisive punitive measure on offending node(s) beyond mere blocking in a MANETs is likely going to foster more cooperation among the participating nodes than the present system. Thus this model has the tendency of improving the performance of the overall network. In this paper, we presented a model that withdraws the life battery of a malicious node on MANETs. The withdrawal of the life battery is a more severe punitive measure than the mere blocking of MAC address(s) of the offending node(s). This punitive measure serves as deterrence against future misbehaviors in the distributed networks. Our model implementation uses the existing IDS iterative scanning of the nodes on the network before CIDM is lunched. This implementation is quite limited to simulation. The model presented is very simple and implementable. Our research effort is to develop a real life system, which will mitigate malicious nodes by making this model possible in distributed system environment. Also, we are looking forward to develop a system that will apportion stiffer punishment to malicious node on in this environment in the nearest future.

References

[1] Agah A., Das S.K., Basu K., Asadi M.: Intrusion detection in sensor networks: a non-cooperative game approach. *Network Computing and Applications, 2004. (NCA 2004). Proceedings. Third IEEE International Symposium on*, pp. 343–346, 2004.

[2] Atassi A., Sayegh N., Elhajj I., Chehab A., Kayssi A.: Malicious Node Detection in Wireless Sensor Networks. *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 456–461, 2013.

[3] Balajinath B., Raghavan S.V.: Intrusion Detection through Learning Model. *Computer Communications*, vol. 24(12), pp. 1202–1212, 2001.

[4] Bayne C.J.: Molluscan internal defense mechanism: The fate of C14-labelled bacteria in the land snailHelix pomatia (L.). *Journal of comparative physiology*, vol. 86(1), pp. 17–25, 1973, ISSN 1432-1351, `http://dx.doi.org/10.1007/BF00694474`.

[5] Boping Q., Xianwei Z., Jun Y., Cunyi S.: Grey-theory based intrusion detection model. *Journal of Systems Engineering and Electronics*, vol. 17(1), pp. 230–235, 2006.

[6] Boukerche A., Machado R.B., Juca K.R., Sobral J.B.M., Notare M.S.: An agent based and biological inspired real-time intrusion detection and security model for computer network operations. *Computer Communications*, vol. 30(13), pp. 2649–2660, 2007.

[7] Cai J., Poch U.: Allocate Fair Payoff for Cooperation in Wireless and Ad-hoc Networks Using Shapley Value. *Proceedings of the 18th International Parallel and Distributed Processing Symposium, IEEE*, pp. 219–226, 2004.

[8] Farrahi V.S., Ahmadzadeh M.: KCMC: a hybrid Learning Approach for Network Intrusion Detection using K-means Clustering and Multiple Classiffiers. *International Journal of Computer Applications*, vol. 124(9), pp. 18–23, 2015.

[9] Geers K.: The challenge of cyber attack deterrence. *Computer Law and Security Review*, vol. 26(3), pp. 298–303, 2010.

[10] Gray R.S., Kotz D., Newport C., Dubrovsky N., Fiske A., Liu J., Masone C., McGrath S., Yuan Y.: CRAWDAD data set dartmouth/outdoor. Http://crawdad.org.

[11] Gupt G.K., Singh J.: Truth of D-DoS Attacks in MANET. *Global Journal of Computer Science and Technology*, vol. 10(15), pp. 15–22, 2010.

[12] Harper J.G.: Traffic violation detection and deterrence: implications for automatic policing. *Applied Ergonomics*, vol. 22(3), pp. 189–197, 1991.

[13] Hoath P., Mulhall T.: Hacking: Motivation and deterrence, part II. *Computer Fraud and Security*, vol. 5, pp. 17–19, 1998.

[14] Kendall J.R.: Deterrence by Presence to Effective Response: Japan's Shift Southward. *Orbis*, vol. 54(4), pp. 603–614, 2010, ISSN 0030-4387, `http://www.sciencedirect.com/science/article/pii/S0030438710000463`.

[15] Kodialam M., Lakshman T.V.: Detecting network intrusions via sampling: a game theoretic approach. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, pp. 1880–1889, 2003, ISSN 0743-166X.

[16] Kolias C., Kambourakis G., Maragoudakis M.: Swarm intelligence in intrusion detection: A survey. *Computers and security*, vol. 30(8), pp. 625–642, 2011.

[17] Larsson T., Hedman N.: Routing protocols in wireless ad-hoc networks – a simulation study. *Lulea University of Technology*, 1998.

[18] Liu Y., Comaniciu C., Man H.: A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks. *Proceeding from the 2006 Workshop on Game Theory for Communications and Networks*, GameNets '06, ACM, New York, NY, USA, 2006, ISBN 1-59593-507-X, `http://doi.acm.org/10.1145/1190195.1190198`.

[19] Lui K., Dang J.V.P.K., Balakrishan K.: An Acknowledgement Based Approach for the Detection of Routing Misbehaviour in MANETs. *IEEE Transactions on Mobile Computing*, vol. 6(5), pp. 536–550, 2007.

[20] Mishra A., Nadkarni K., Patcha A.: Intrusion Detection in Wireless Ad-hoc Networks. *IEEE Wireless Communication*, vol. 11(1), pp. 48–60, 2004.

[21] Ning P., Cui Y., Reeves D.S.: Constructing Attack Scenarios Through Correlation of Intrusion Alerts. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, pp. 245–254, ACM, New York, NY, USA, 2002, ISBN 1-58113-612-9, `http://doi.acm.org/10.1145/586110.586144`.

[22] Obaidat M.S., Woungang I.: *Pervasive Computing and Networking.* John Wiley and Sons, 2011.

[23] Orfila A., Carbo J., Ribagorda A.: Autonomous Decision on Intrusion Detection with Trained BDI Agents. *Computer Communications*, vol. 31(9), pp. 1803–1813, 2008.

[24] Polla M.L., Martinelli F., Sgandurra D.: A Survey on Security for Mobile Devices. *IEEE Communications Surveys Tutorials*, vol. 15(1), pp. 446–471, 2013, ISSN 1553-877X.

[25] Saxena H., Richariya V.: Intrusion Detection in KDD99 Dataset Using SVM-PSO and Feature Reduction with Information Gain. *International Journal of Computer Applications*, vol. 98(6), pp. 25–29, 2014.

[26] Senbel S.A., Ibrahim A., Zaki E.A.: Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol. *Journal of Computer Sciences and Applications*, vol. 3(4), pp. 90–93, 2015.

[27] Senthilnayaki B., Venkatalashmi K., Kannan A.: Intrusion Detection System using Feature Selection and Classification Techique. *International Journal of Computer Science and Application (IJCSA)*, vol. 3(4), pp. 145–151, 2014.

[28] Shakshuki M., Kang N., Sheltami T.R.: EAAK A Secure Intrusion-Detection System for MANETs. *IEEE Transactions on Industrial Electronics*, vol. 60(3), pp. 1039–1098, 2013.

[29] Shamshirband S., Anuar N.B., Kiah L.M., Patel A.: An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. *Engineering Applications of Artificial Intelligence*, vol. 26(9), pp. 2105–2127, 2013.

[30] Subba B., Biswas S., Karmakar S.: Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. *Engineering Science and Technology an International Journal*, vol. 19, pp. 782–799, 2016.

[31] Thaseen I.S., Kumar C.A.: Intrusion detection model using fusion of chi-square feature selection and multi class {SVM}. *Journal of King Saud University - Computer and Information Sciences*, 2016, ISSN 1319-1578, `http://www.sciencedirect.com/science/article/pii/S1319157816300076`.

[32] Wang Q., Borisov N.: Octopus: A Secure and Anonymous DHT Lookup. *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*, pp. 325–334, 2012, ISSN 1063-6927.

[33] Wang W., Guan X., Zhang X.: Processing of massive audit data streams for real-time anomaly intrusion detection. *Computer communications*, vol. 31(1), pp. 58–72, 2008.

Affiliations

Emmanuel A. Olajubu

Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria, `emmolajubu@oauife.edu.ng`

Abiodun Akinwale
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria, `logicstronics@yahoo.com`

Kazeem Ibraheem Ogundoyin
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria, `logicstronics@yahoo.com`

Received: 25.01.2016
Revised: 8.06.2016
Accepted: 9.06.2016