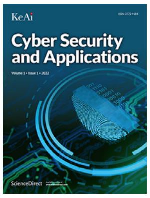
Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/



Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory

S Vijayalakshmi [a], S Bose [b], G Logeswari [b,*], T Anitha [b]

[a] Department of Computer Science and Engineering, Government College of Engineering, Erode (IRTT), Tamil Nadu, India
[b] Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai, Tamil Nadu, India

ARTICLE INFO

Keywords:
Ad hoc networks
Intrusion detection
Game theory
Game engine
Reactive game
Proactive game
Packet dropping attack
AODV

ABSTRACT

Ad hoc networks are a new perspective of wireless communication for versatile hosts. Security is a colossal worry for ad hoc networks, especially for those security-touchy applications. The huge highlights of ad hoc networks cause both difficulties and openings in accomplishing security objectives. One such aim is to consider the assaults from within the system by compromised nodes correspondingly as to consider harmful assaults propelled from outside the system. Designing an Intrusion Detection System (IDS) that suits the security needs and characteristics of ad hoc networks for viable and proficient performance against intrusions is one potential solution to vanquish vulnerabilities. This paper examines a genuine and hurtful attack called, “Malicious Packet Dropping Attack” in the network layer. To secure against this attack, a novel methodology utilizing game theory is proposed. The proposed system monitors the conduct of the neighbor nodes and conquers the demerits such as false positives present in traditional IDS, thereby providing secure correspondence between nodes that communicate with one another to course the traffic from source to destination. With the existence of malicious nodes, the proposed system has accomplished a 42% increase in the packet delivery ratio.

1. Introduction

1.1. Mobile Ad hoc networks

Mobile Ad hoc Networks (MANET), as the name recommends, have no supporting framework. It is a self-governing distributed framework that comprises various portable nodes associated with remote connections, forming discretionary time-varying wireless network topologies. It is not simpler to achieve security in the MANET due to reasons such as deficient physical assurance of every node, the sporadic nature of connectivity, the absence of accreditation authority, and the absence of a concentrated administration unit. An Intrusion prevention system is not guaranteed to work constantly, and this underscores the requirement for intrusion detection as a significant area of research in Ad hoc network security [1].

1.2. Intrusion detection system

The illicit and abusive usage of a computer system is identified by Intrusion Detection System (IDS). This system cautions when an intruder is recognized. The system contains the following phases

(i) Monitoring
(ii) Analysis
(iii) Response

IDS can be characterized in many ways

(i) Anomaly and/or Signature Based
(ii) Host and/or Network Based
(iii) Proactive and/or Reactive Systems.

A misuse detection system, otherwise called signature-based IDS distinguishes intrusions by looking for patterns of traffic or application information ventured are malevolent. Anomaly-based IDS recognizes intrusions by informing operators of traffic or application content ventured to be different from the expected action on the network or host. Anomaly-based IDS typically accomplishes this with self-learning [2].

A network intrusion detection system screens numerous hosts and investigates network traffic to recognize the intrusions [29]. The network traffic is accessed by interfacing a hub, network switch configured for port mirroring, or network tap [3]. On the other hand, a host-based intrusion detection system distinguishes intrusion by investigating system calls, application logs, file-system modifications, other host activities, and states [25,26].

IDS can be proactive and/or reactive. The reactive mechanism strives to alleviate the impact of an attack on the victim, so they detect the

[*] Corresponding author.
E-mail address: logeswarig4@gmail.com (G. Logeswari).

https://doi.org/10.1016/j.csa.2022.100011
Received 30 August 2022; Received in revised form 17 October 2022; Accepted 23 November 2022
Available online 26 November 2022

attack and respond to it [30]. Proactive mechanisms attempt to predict future behavior and take defensive actions before the actual attack is going to be launched.

1.3. Game theory

Game Theory is an investigation of correspondence between at least two substances with opposing or varied interests. It is used to develop quantitative analysis techniques for Network and Information Security as it provides a natural vehicle for a rigorous formulation of attacks, threat analysis, and reactive decision-making [4]. It involves the study of planned circumstances where players choose different actions in an attempt to amplify their returns and a provides decision control framework for the IDS. Games can be Stochastic or Bayesian games. In the Stochastic (Repeated) game, the assault activities are associated and known with sureness. While in Bayesian games, the data about the qualities of different players (i.e. payoffs) is inadequate and assault activities are assumed to be uncorrelated. In this paper, both reactive and proactive game theoretic methodologies are utilized to recognize and protect against malicious nodes/attacks from the network.

1.4. Attack types

Malicious nodes may take the advantage of inherent traits of ad hoc to launch different kinds of attacks. Black hole attacks, replay attacks, message tampering, wormhole attack, rushing attack, and packet drop are several possible attacks in the network layer [5].

This work centers around a malicious packet-dropping attack, in which a node maliciously drops the packet as an alternative to forwarding it. Network throughput will decrease significantly in the presence of malicious nodes. In this paper, a host-based misuse detection system using game theory approaches is implemented to perceive the malicious nodes and furnish security to the network.

1.5. Overview of the AODV protocol

The Ad hoc On-Demand Distance Vector Routing Protocol is a receptive routing protocol in which routes are possibly established when expected to lessen traffic overhead [6]. AODV is intended for networks with tens to thousands of versatile nodes. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are message types characterized by AODV. The AODV starts a route revelation procedure to find the destination node when the source node needs a course to a destination. The source node floods the network with a route request packet (RREQ), requesting a route to be set up to the destination. The transitional node restores its routing table for an inverted route to the source on receiving an RREQ. With an ascent in hop count, all the receiver nodes which don't have a path to the destination transmit the RREQ packet to their neighbors. When the RREQ query reaches either the destination or any other intermediate node that has a current route to the destination, a route reply (RREP) is sent back to the source node [26]. AODV manages the routing table. Every node has a routing table. The node sends a route reply to the source node when it knows the route to the destination [27]. Its entries are:

- Destination IP Address
- Prefix Size
- Destination Sequence Number
- Next Hop IP Address
- Lifetime
- Hop Count
- Network Interface
- Other state and routing flags

The AODV protocol does not contain any security mechanism, such as strong authentication. To initiate assaults on AODV, hop count fields and sequence numbers are utilized. In this way, mischievous practices such as MAC spoofing, IP spoofing, dropping packets, or altering the contents of control packets cannot be adverted. Few attacks against AODV can be prevented by using protocols such as SAR and SAODV with a cost of performance in terms of overhead and latency.

Several attacks such as black hole attacks, wormhole attacks, and rushing attacks are possible in the network layer [7].

The ability of nodes in MANETs to collaborate with neighbors to disseminate data is one of their most essential characteristics. Malicious nodes exploit this functionality to work with normal nodes to disrupt network operations and reduce network efficiency. These nodes attack other network nodes and avoid detection by using the mobility of nodes in MANETs. One of the more effective techniques is to use game theory to detect malicious nodes.

In this paper, a portion of the vulnerabilities, explicitly assaults against AODV such as malicious packet drop is analyzed. To distinguish attacks on AODV, a solution using the neighbor monitoring technique and game theory is proposed. To give optimal strategies for anomaly-based intrusion detection systems, the game theoretical analysis method is proposed.

The rest of this paper is organized as follows: Section 2 illustrates the related work for MANET that is based on game theory. Section 3 explains the proposed Intrusion Detection System using Game theory. Section 4 gives the results and discussion of the proposed work. Section 5 gives the conclusions and future enhancements.

2. Related work

Watchdog and Path rater are two extensions to the DSR algorithm, proposed by Marti et al. [8]. The misbehaving nodes are identified by the watchdog by monitoring the next node transmission. The path rater uses the data from the watchdog extension to choose a path that is most probable to deliver packets. The path rating is computed by averaging the rating of the nodes in the path, where every node maintains a rating for all the nodes it knows in the network. The principle drawback is that the misbehaving nodes are not rebuffed and there are no incentives for the nodes to coordinate.

CONFIDANT protocol and a range of enhancements are presented by Buchegger et al. [9]. Each node monitors the conduct of its next-hop neighbors. The data is given to a reputation system which updates the rate of the nodes. Based on the rating, a trust manager makes decisions about providing or accepting route information, accepting a node as part of a route, and similar decisions. A node notifies its friends by forwarding an ALARM message if it assumes its neighbor node to be misbehaving. The information is transmitted to a path manager if the rating of the node is intolerable. All the routes containing the intolerable node are deleted from the path cache. The principle disadvantage of this methodology is the spreading of false reputation ratings by malicious nodes present in the network.

CORE scheme and different related issues were portrayed by Michiardi et al. [10]. In this scheme, each node calculates a reputation value for its neighbor nodes. The reputation mechanism varies between subjective reputation, indirect reputation, and functional reputation. By staying away from the spread of negative ratings, the mechanism resists attacks such as denial of service. The misbehaving node service is suspended when a neighbor's reputation decreases less than a predefined value. This paper also suffers from the same drawback as mentioned in the watchdog mechanism [8,9].

Banal et al. [11] proposed a novel methodology called OCEAN for robust packet forwarding. This method is based on the node's perceptions. Each node depends on its data and rating is not exchanged. Hence trust management is not necessary. The rating is based on a counter that calculates steps a node performs and based on a faulty threshold, the node is appended to a faulty list. For route selection, a node appends an avoid list to every RREQ, and based on this list, an RREP is generated. A second-chance method is offered to give nodes that were previously considered mischievous another opportunity to operate. The main disadvantage of the system is that the malicious nodes are given a second chance to operate. So the malicious nodes keep on attacking the network.

Cooperative and reliable packet forwarding proposed by Anker et al. [12], addresses the issue of client cooperation in especially ad hoc networks. Past examinations, depending on reputation systems, have shown solutions designed for Dynamic Source Routing (DSR) protocol. This paper features various aspects of cooperation enforcement and reliability when AODV is the underlying protocol. The downside is that negative ratings can be spread by malicious nodes in an endeavor to diminish other node's reputations.

Sakthivel et al. [13]. proposed a secure routing framework that prevents routing misbehavior attacks in the presence of malicious nodes. This method uses an acknowledgement scheme that adds dummy packets to the real payload traffic. This framework validates the existence of malicious nodes by monitoring the dropping of dummy packets and depends on the trust mechanism to remove the misbehaving nodes in the critical path.

Sen [14] presents an in-depth survey on a variety of security and privacy-related problems in Wireless Mesh Networks. Das et al. [15]. proposed a game-theoretic model which identifies selfish nodes in MANETs. This model guarantees secure data transfer at a low cost in minimum idle time. This model failed to consider the existence of malicious nodes.

Taheri et al. [16]. presented an approach that detects malicious nodes using game theory. The malicious nodes are identified by game components, sent and received data as well as considering the data which has been stored in different stages. Wang et al. [17]. proposed a novel Mean Field Game Theoretic approach to enhance security in cognitive radio MANETs. This approach improves the lifetime of MANET and also reduces the possibility of compromising.

A new hybrid acknowledgement approach is proposed by Bounouni et.al [18]. This approach aims to motivate the selfish nodes to assist in the route discovery process and to punish the malicious nodes. To evaluate the trustworthiness of each node, a novel reputation computation method is proposed. In this method, the nodes having low reputation value are penalized and it chooses trustworthy forwarding paths. This approach reduces the malicious drop ratio and improves the throughput.

The security for decision-making in Ad hoc sensor networks is provided by trust and reputation- based approaches. Ahmed et al. [19] presented a literature survey on various trust and reputation-based approaches. The trust model is categorized into two namely, node-centric and system-centric models. Unresolved issues of trust and reputation management have been identified. Intrusion detection for mobile ad hoc networks is complex because of its dynamic nature and lack of centralized monitoring points. The issue of intrusion detection for MANET is presented by Şen et al. [20]. This paper also discusses the various solutions being proposed earlier.

Janusz et al. [21]. presented the commonly used algorithms such as swarm intelligence, evolutionary algorithms, artificial immune systems, and evolutionary games to improve cyber security in MANETs. This paper also discusses the basic defense mechanisms in MANETs for intrusion detection and prevention. Subba et al. [22] proposed a framework that identifies malicious nodes by using lightweight neural networks and specification rules. A reputation update and expulsion mechanism based on Shapley value and Vickery Clark Grooves (VCG) have been proposed to support cooperation and discourage malicious behavior among monitoring nodes. This approach has achieved a higher detection rate over several attacks.

Ganapathy et al. developed a new intelligent Conditional Random Field (CRF)-based feature selection approach to develop a novel intrusion detection system that optimizes the number of features [31]. Furthermore, to accomplish classification with these reduced data, an existing Layered Approach (LA) based method is applied. To distinguish and classify anomalous behavior from normal behaviors in the Internet of Things depending on the type of attack, Reddy et al. proposed an innovative deep learning-based framework with a dense random neural network approach [32]. This research focuses on a thorough analysis of experimentation performance and evaluations of deep learning neural network architecture for the identification of seven category attacks. This research presented a bidirectional long-term and short-term memory network based on the multi-feature layer to address the low-frequency and multi-stage attacks in IIoT. To properly identify attacks with various intervals, sequence and stage feature layers are first incorporated in the training phase [33]. These layers may learn the appropriate attack interval using previous data. The detection model is then updated with the introduction of a double-layer reverse unit.

In an IoE environment, Bera et al. [34]. examine numerous attack tendencies. The evolution of blockchain technology in the Internet of Everything is then discussed. To safeguard the Internet of Everything, a blockchain-envisioned access control system powered by artificial intelligence has been proposed. The pre-detection phase of quick detection and the deep detection phase of deep detection are combined in the efficient detection framework suggested by Lu et al. [35]. The Android application package (APK) is carefully examined, and features like permissions and opcodes that can tell a benign APK from a malicious one are swiftly extracted. In addition, the convolutional neural network (CNN), which automatically extracted the hidden pattern inside features, is picked for feature selection to acquire the feature subset that can identify the attributes most effectively

3. System architecture

The intermediate nodes are used to forward the packets from the source to the destination. While forwarding, the intermediate nodes maliciously drop the packets.

Abderrahmane et al. [23] proposed a novel approach to authenticating the proper forwarding of packets by an intermediate node. Mohanapriya et al. [24] has proposed a lightweight, energy- efficient, and non-cryptographic intrusion detection framework to detect gray-hole attacks in MANET. The drawback of this scheme is that it consumes high power for operating the intrusion detection system. The fundamental objective of the research was to identify a methodology that updates network security. From the survey related to security in MANET, it was discovered that game theory-based approaches were predominantly being utilized to take care of different issues related to MANET.

The overall architecture of our system is shown in Fig.1. There are four modules. They are the neighbor monitoring module, neighbor trust module, game engine module, and packet forwarding module. In this architecture, every node in the network monitors the behavior of its neighbor. Based on the observed behavior, the nodes update the trust value for each of its neighbors. The trust value is the ratio of the number of the packet forwarded by the neighbor to the number of packets sent to it. Game theory techniques are used by each node for decision-making purposes. There are two game strategies used. They are reactive strategy and proactive game models. A reactive game strategy provides the best move, the node could make under a given situation using a different game strategy such as TFT, Pavlov. Using a proactive game strategy, nodes could predict the neighbor's future behavior using the prisoner's dilemma game model.

3.1. Monitoring module

The monitoring module monitors the behavior of the neighbor nodes. Whenever a node sends a packet to another node, it initially captures the packet in its buffer until a timeout occurs. It then monitors whether the neighbor node forwards that packet or not. This is called the promiscuous mode monitoring technique. If the neighbor node forwards the packet, then the node increments the forward counter and updates the recent move of the neighbor node as cooperate. This is shown in Fig.2.

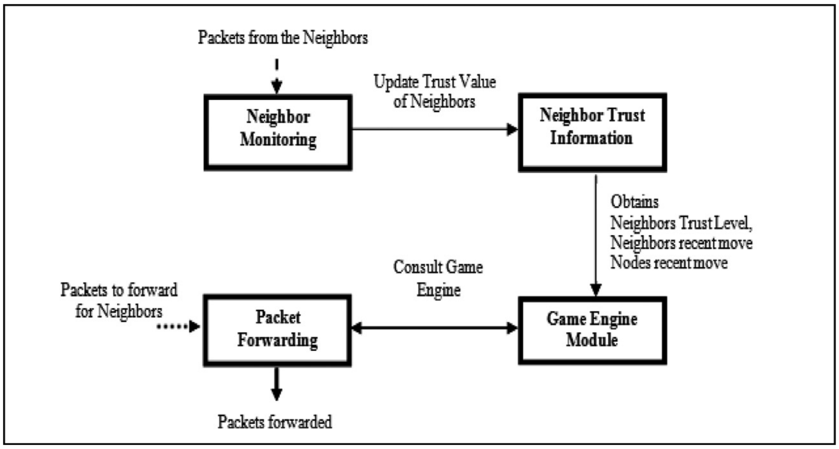


Fig. 1. Architectural Design.

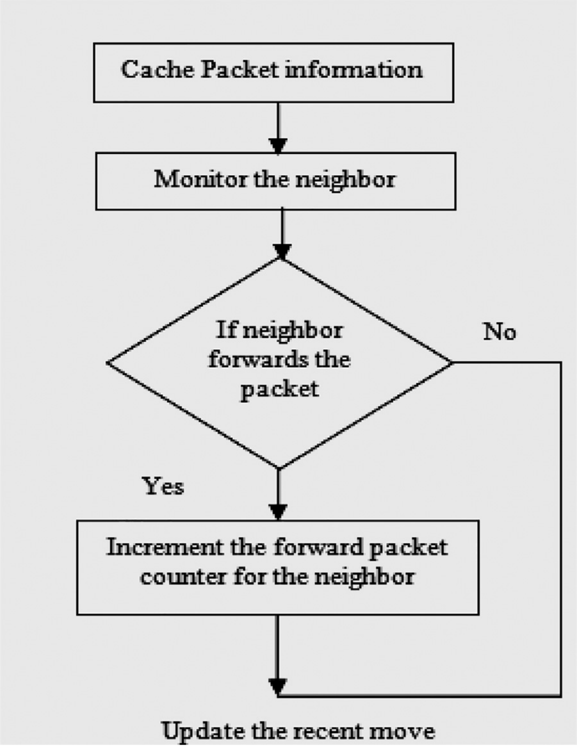

Cache Packet information
Monitor the neighbor
If neighbor forwards the packet
No
Yes
Increment the forward packet counter for the neighbor
Update the recent move

Fig. 2. Monitoring Module.

Algorithm	
1.	Tap the packets forwarded by the neighbors.
2.	Check whether the packet is present in the forward cache of the node.
3.	If the packet is present in the cache, then increment the number of packets forwarded in the neighbor's trust table.

3.2. Neighbor trust information

Every node in the network has to trust information about its neighbor. This information is stored in the neighbor trust table. It contains the following fields as shown in Table 1.

3.3. Game engine

The goal of the game engine is to encourage independent, competitive players to make the best decisions possible in a strategic context. If the opponent node's move is known, the game engine provides the best decision to defend against the opponent's move. In this work, two game theoretic strategies such as reactive and proactive strategies are applied. Reactive strategies provide the best move based on different gaming strategies whereas the proactive approach predicts the node's future behavior. If the predicted move of the node is cooperating, then the packet is forwarded to the node otherwise the packet is not forwarded to that node.

Table 1
Neighbor Trust Table.

1	Neighbor id (e.g. Node 2)
2	Neighbor's recent move against the node (e.g. C/D-Cooperate/Defect)
3	Node's recent move against neighbor (e.g. C/D)
4	No. of packets sent by the node to the neighbor (e.g. 4)
5	No. of node's packets forwarded by the neighbor (e.g. 3)
6	No. of packets sent by the neighbor to the node (e.g. 4)
7	No. of neighbor's packets forwarded by the node (e.g. 3)
8	Forward Rate (e.g. 0.75)
9	TTL to update (e.g. 1,067,167,598)

3.3.1. Trust class

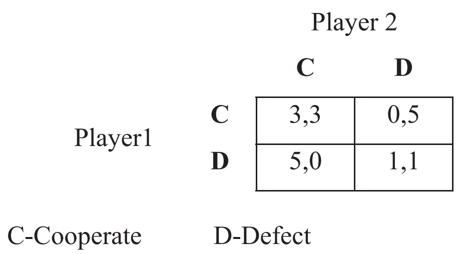
Nodes in the network calculate the trust value for their neighbor periodically. Trust value is the ratio of the number of packets forwarded by the node to the number of packets sent to it. A Trust class is assigned to each node based on the trust value computed previously. If the forwarding rate is greater than THRESHOLD1 (0.7) then the trust class of the node is one (CLASS 1). If the forwarding rate is between THRESHOLD1 (0.7) and THRESHOLD2 (0.3), then the trust class of the node is two (CLASS 2). If the forwarding rate is less than THRESHOLD2 (0.3), then the trust class of the node is three (CLASS 3). Nodes in trust class 3 are termed as malicious and no packet is sent to that node. The threshold value of 0.7 is assumed to be the maximum threshold value because a higher value (0.9) would lead to false negatives. For example, if a new node joins the network and 4 packets are sent to the node. If the node initially forwards the first 3 packets, then its forwarding rate at that moment will be 0.75. Since the value is greater than the maximum threshold value (0.7), no problem occurs. But if the threshold value is chosen as 0.9, then the rating assigned to the node will be bad even though the node is not a malicious nodes.

1. CLASS 1 (Points: 3)

   If Forwarding Rate > THRESHOLD1

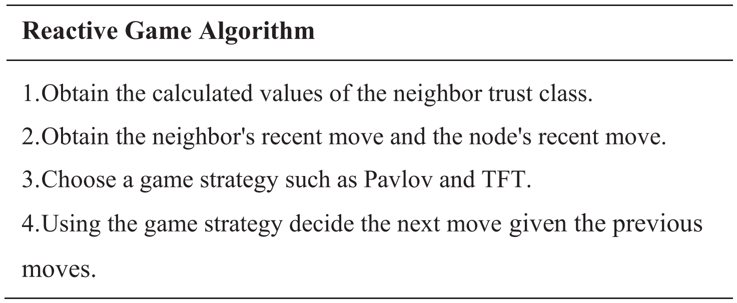
2. CLASS 2 (Points: 2)

Table 2
Reactive Game.



		Player 2	
		C	**D**
Player1	**C**	3,3	0,5
	D	5,0	1,1

C-Cooperate D-Defect



Reactive Game Algorithm

1.Obtain the calculated values of the neighbor trust class.

2.Obtain the neighbor's recent move and the node's recent move.

3.Choose a game strategy such as Pavlov and TFT.

4.Using the game strategy decide the next move given the previous moves.

If THRESHOLD1> Forwarding Rate >THRESHOLD2

3. CLASS 3 (Points: 1)

   If Forwarding Rate < THRESHOLD2

- THRESHOLD1 = 0.7
- THRESHOLD2 = 0.3

3.3.2. Reactive game

A reactive game strategy provides the best move for the node given the recent move of the node and neighbor. The next move is chosen based on different game strategies (TFT, PAVLOV).

TFT: Repeat the previous move of the neighbor.

Pavlov: If both the previous moves are cooperative, then choose to cooperate in the next move. If either of the previous moves is defective, then choose to defect in the next move. Decide the next move based on,

1. Neighbor's Trust Class
2. Neighbor's last move
3. Node's last move

For example, if the trust class calculated for the neighbor is 2 (forwarding rate between 0.7 and 0.3) and the node has recently sent a packet to the neighbor node(C-cooperate) and the neighbor has recently forwarded that packet(C), then the best decision for the node is to cooperate with the neighbor. This is shown in Table 2.

3.3.3. Proactive game

To determine whether a user is an intruder, a proactive game strategy directs the user's behavior and monitors it in various contexts. A proactive game strategy predicts the neighbor's next move based on the previous history. The next move is predicted based on the following factors:

- Node's recent move is m and the neighbor's recent move is n.
- Trust value is calculated using the previous behavior and payoff matrix.
- If ***trust value*** > THRESHOLD, then predict the Neighbor's next move as C (COOPERATE), otherwise, D (DEFECT).

```
Proactive Game Algorithm

Nodes recent move be m and neighbors recent move be n.
1.  Trust value is calculated using the formulae
Trust value = trust class points * payoff(n,m)
2. If trust value > THRESHOLD then, predict the
Neighbor's next move as C, otherwise, D.
```

Payoff Matrix

The outcome of a player's decision in a game can be expressed using a payoff matrix. The payoff matrix is used to compute the payoff value for the node and neighbor at each phase of the game. Payoffs are numbers that signify the inspiration of players. It represents the utility values for each action made by the players. The payoff matrix is represented using the prisoner dilemma game model as shown in the following Table 3.

Prisoner's Dilemma

The Prisoner's Dilemma is a decision model. In this model player 1 and player 2 are arrested for espionage and located in separate cross-examination rooms. Each player has the choice to cooperate with his peer or to defect against him. Both players are rewarded with a sentence of length R if they cooperate (C), and both obtain a penalty P if defect (D). If one player defects and the other cooperates, the defector obtains the best payoff (or temptation payoff) T for exploiting his opponent.

The adversary is penalized with the sucker payoff S, the worst likely result. Here, we declare [R, S, T, P] = [3, 0, 5, 1]. The payoff matrix for this game, representing the points received by each player in each situation, is shown in Table 3.3 (scores listed as [player 1, player 2]).

Nash Equilibrium depicts what move every player will make to augment his/her score based on correct assumptions about the other player's activities. In the prisoner's dilemma, regardless of what one player does, the other player will be better off defecting. If player 1 cooperates, player 2 can get 5 points for defecting rather than 3 for cooperating. If player 2 defects and player 1 also defects, then he can get a score of 1 rather than 0. Each player will utilize this logic, leading to a Nash Equilibrium of (Defect, Defect). If both players were to alter their moves to Cooperate, they each would triple their score.

Table 3
Payoff Matrix.

Class	1	1	1	1	2	2	2	2	3	3	3	3
Neighbor's recent move	D	D	C	C	D	D	C	C	D	D	C	C
Node's recent move	D	C	D	C	D	C	D	C	D	C	D	C
Node's next move	C	C	C	C	C	D	D	C	C	D	D	C

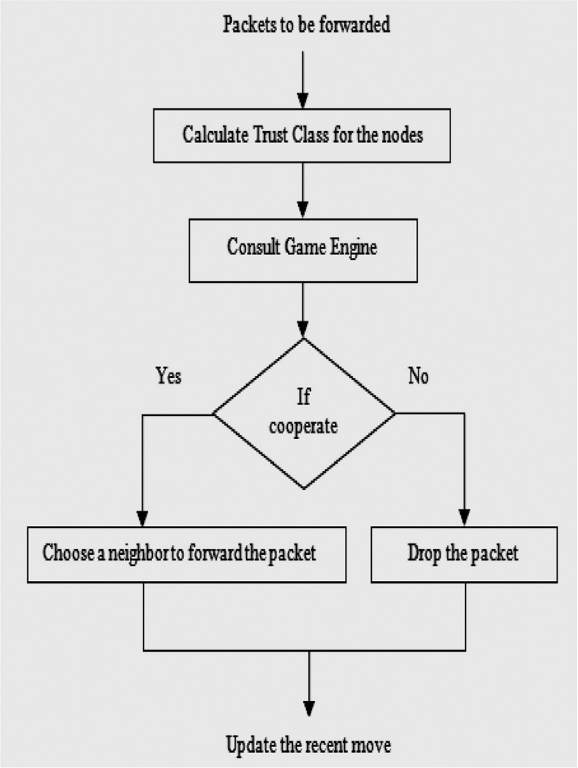


Fig. 3. Forwarding Module.

3.4. Packet forwarding module

The forwarding module forwards or drops the packet based on the result of the game engine. If the result of the game engine is cooperating (Forward), then it chooses the most trustworthy neighbor and forwards the packets to it. If the result of the game engine is a defect, then it drops the packet instead of forwarding it which is shown in Fig.3.

Packet Forwarding Algorithm

```
1.   Consult the game engine to decide whether to forward the
     packet from the neighbor or drop the packet.
2.   If the result of the game engine is cooperate then choose a
     neighbor to forward the packet.
3.   Forward the packet to that neighbor.
4.   If the result of the game engine is defective, then drop the
     packet from that neighbor.
5.   Update the recent move of node and neighbor.
```

4. Performance analysis

The performances of MANET are analyzed based on the packet delivery ratio, the total number of packets generated, the number of dropped packets, and the number of received packets. The following metrics are used [28].

Table 4
Simulation Environment.

Simulation environment	Simulation value
Simulation Area	800×600
Node Movement	Random Waypoint model
Radio range	250 m
Number of nodes	10–25
CBR connections	10–50
Packet sizes	512–2000 bytes
MAC protocol	IEEE 802.11
Routing protocol	AODV
Transport Layer	TCP
Initial energy	10 J
Transmission power	0.3 to 3 mW
Reception power	0.6 to 4 mW
Simulation Time	20 to 100 S

Packet delivery Fraction: This is the fraction of the data packets generated by the CBR sources that are delivered to the destination.

Routing Load: This is the ratio of overhead packets to delivered control packets corresponding to the particular node.

False Positives: This is the ratio of the number of nodes to the percentage of false positives. The false positive rate is defined as the ratio of the number of non-malicious nodes falsely identified as malicious to the total number of normal events.

5. Results and discussion

5.1. Simulation environment

The simulation was conducted on the platform of Network Simulator (ns-2.28), an object-oriented, discrete event-driven network simulator developed at Berkeley and written in C++ and OTcl.

5.2. Graphical results with discussion

In the case of a collision attack, the performance is calculated as the number of nodes vs. the percentage of false positives which is shown in Fig.4.

When the number of nodes increases, the percentage of false positives also increases. This is because when the numbers of nodes are farther apart, then the nodes within the transmission range of the adversary node are fewer.

Table 4 lists the ns-2 parameters in our simulation. We simulated with different configurations such as 10, 15, 25, and 40 nodes distributed over 670 × 670 and 800 × 600 to obtain performance. The simulation is carried out for 20 to 100 s. Packets among the nodes are transmitted with a constant bit rate (CBR) of four packets per second.

False positives are also less. In the case of 5 nodes, this condition applies. Whereas in the case of 25, 40, and 55 nodes more nodes are closer to each other and they are within the transmission range of the intruder. As a result, the false positives are also high. In the same way,

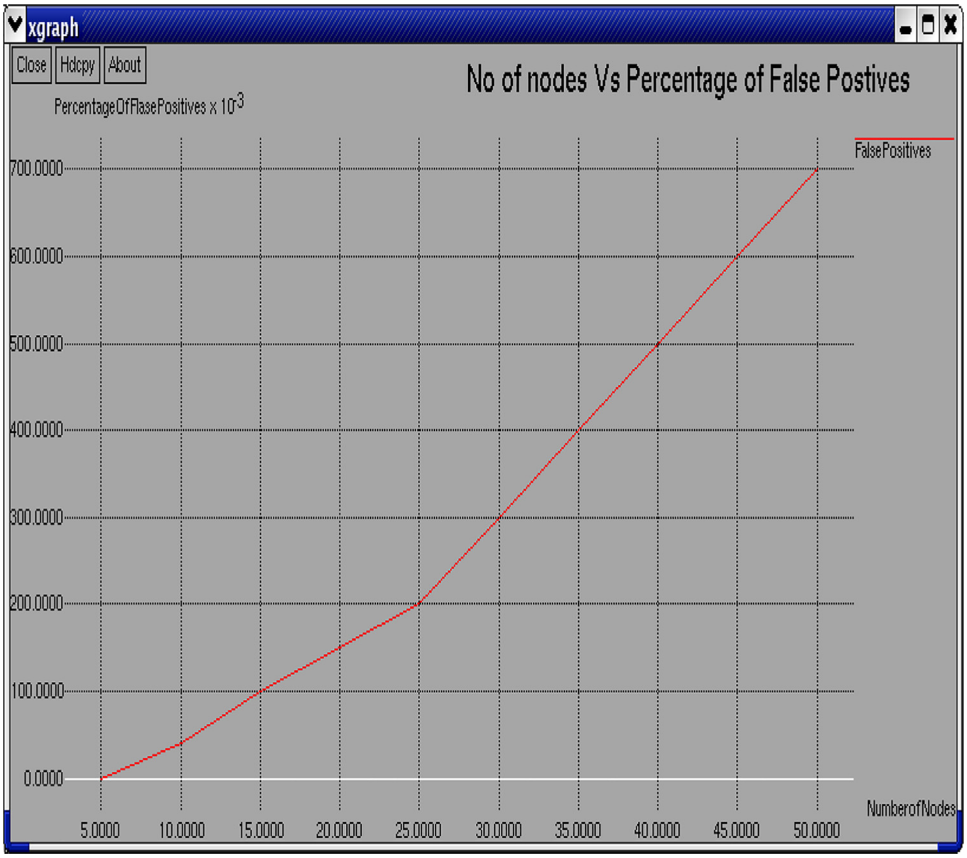


Fig. 4. Number of nodes vs. Percentage of false positives.

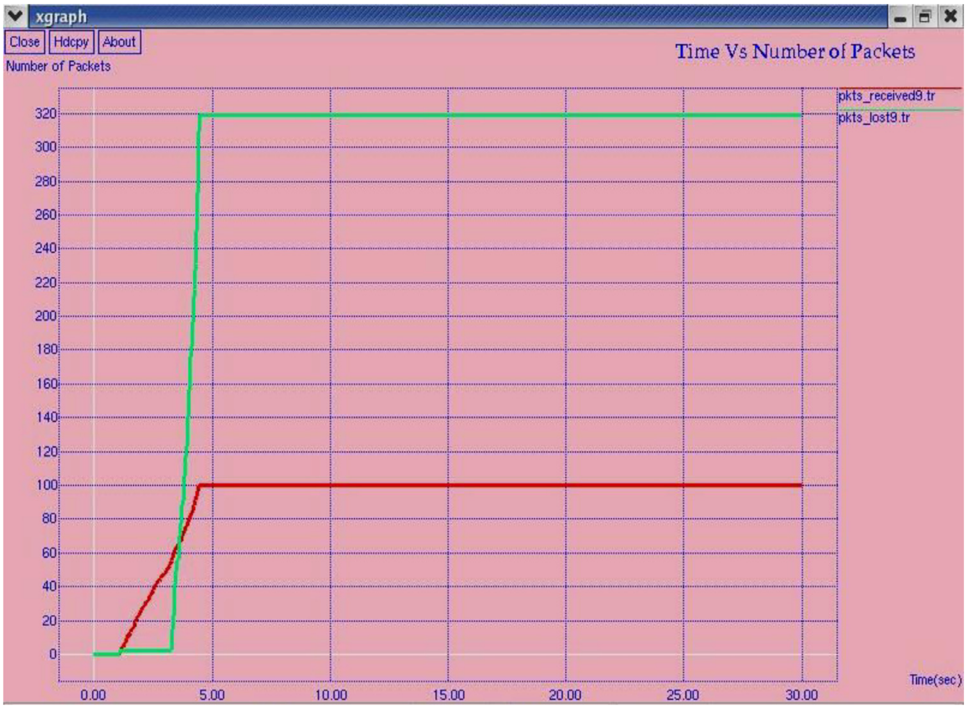


Fig. 5. Time vs. Packets Transmitted.

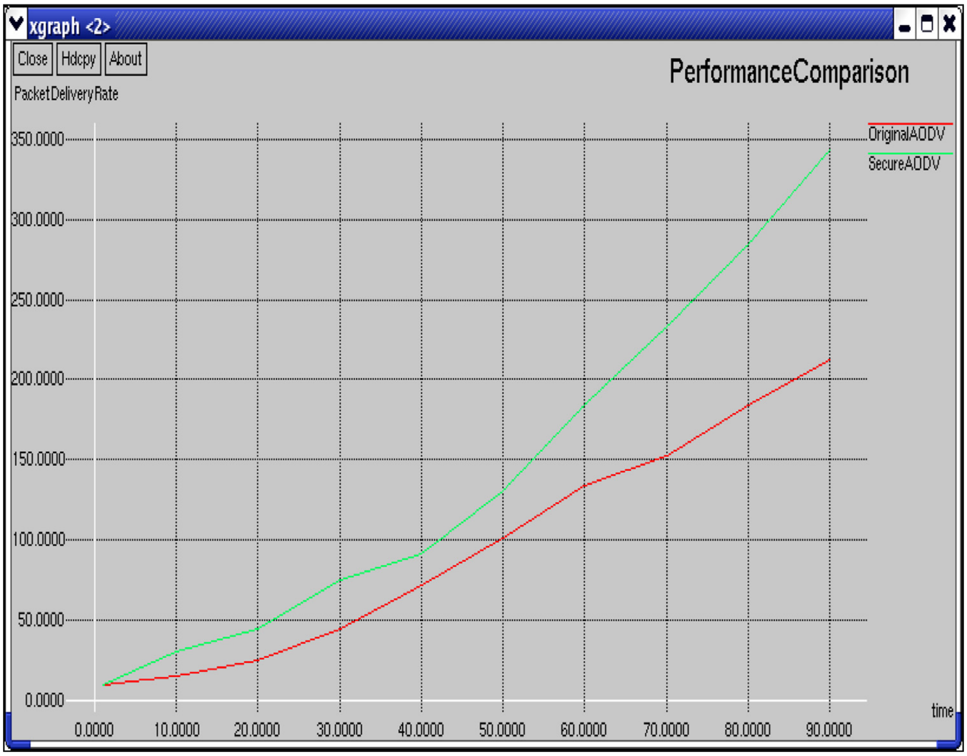


Fig. 6. Performance Comparison.

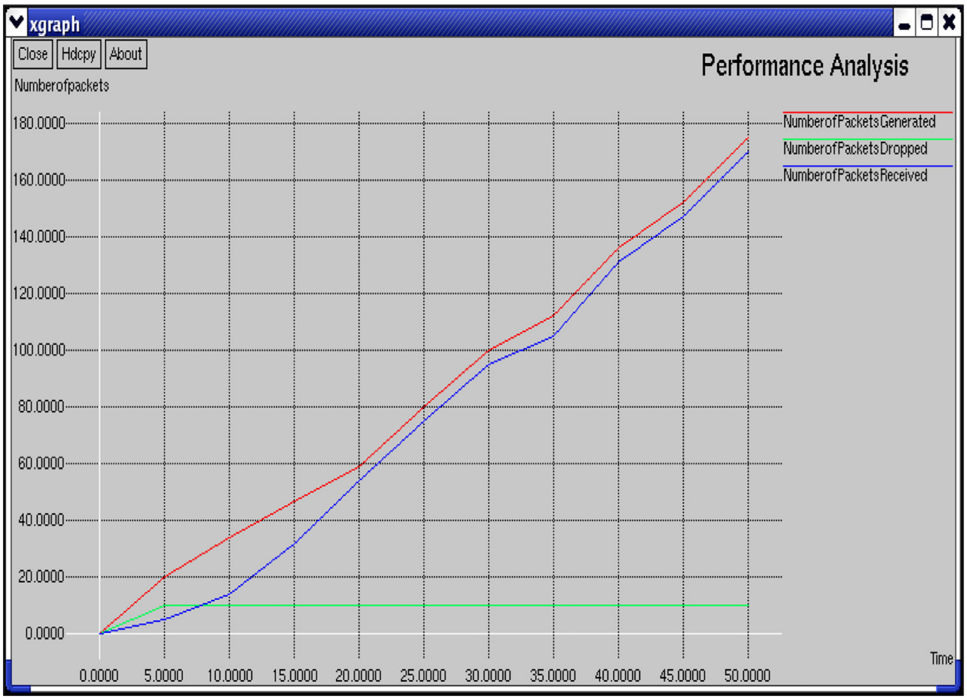


Fig. 7. Number of packets reached vs. Dropped.

the scenario can also be considered as follows, more nodes that are far away from each other with only some of the nodes lying in the transmission range. In such circumstances, false positives are very less. This might also occur. It depends on the configuration of nodes and the transmission range of the neighbor nodes.

For packet drop attack Fig.5, shows the number of packets received, dropped, packet flow start time, end time, and occurred time after the detection process was completed.

The following Fig.6 depicts the performance comparison of the AODV protocol with malicious nodes after detecting and eliminating the malicious nodes.

The results show that the packet delivery rate is increased by 42% in the presence of malicious nodes when compared to the original AODV.

The following graph in Fig.7 shows the total number of packets generated, the number of packets that successfully reached the destination, number of packets dropped by the malicious nodes.

6. Conclusion and future work

The malicious packet-dropping attack agitates the performance of the whole network and refuses service to the destination. To moderate these attacks, a host-based misuse detection system using game theory is utilized to adequately perceive these attacks by monitoring the neighbor nodes in the network. Therefore, our methodology has led to an increase in the packet delivery rate by 42% in the presence of malicious nodes because malicious nodes are recognized at the beginning and eliminated from the network.

More robust security can be provided by identifying collisions between different attacking nodes. Our work is dedicated to AODV and can be adapted to other routing algorithms. In this work, we focus mainly on partial and complete dropping which addresses other patterns of misbehavior in the forwarding phase. It can be improved by dynamically changing the rating policy, to efficiently handle the different patterns of traffic. For future research, additional mechanisms are needed to support QoS and to increase fairness in the network.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Banshilal Patidar, Pinaki A.Ghosh, Intrusion Detection in Wireless Ad Hoc Networks, J. Inform. Secur. Res. 1 (2010) 111–117.

[2] S. Vijayarani, S. Maria, Intrusion Detection System – A Study, Int. J. Secur. Priv. Trust Manage. (2015) 31–44.

[3] Surabhi Thukral, Rutha Maqsood, Divya Upadhyay, To Design an Intrusion Detection System based on Honeypot using Mobile Agent and IP Traceback Technique, Int. J. Sci. Res. (IJSR), India 2 (4) (2013) 196–199.

[4] Xiannan Liang, Yang Xiao, Game Theory for Network Security, IEEE Commun. Surv. Tutor. 15 (1) (2013) 472–486.

[5] Saritha Reddy Veena, Ranesh Babu Inampudi, A Survey on Security Attacks in Mobile Ad Hoc Networks, Int. J. Comp. Sci. Inform. Tech. 7 (1) (2016) 135–140.

[6] Vaishali Sahu, Ashish Roberts, Mahendera Srivastava, An Overview of ADOV Routing Protocol, Int. J. Mod. Eng. Res. 2 (3) (2012) 728–732.

[7] Anil Sainil, Analysis of Security Attacks and Solution on Routing Protocols in MANET, Int. J. Comp. Sci. Mob. Comput. 5 (6) (2016) 182–189.

[8] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, in: Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking, 2006, pp. 255–265.

[9] S. Buchegger, J.Y. Le Boudec, Nodes bearing grudges: towards Routing Security, Fairness, and Robustness in Mobile Ad hoc Networks, in: Proceedings of the IEEE International Conference on Distributed and Network-based Processing, 2005, pp. 223–256.

[10] P. Michiardi, R. Molva, Preventing Denial of Service and Selfishness in Adhoc Networks, in: Proceedings of Working Session on Security in Ad Hoc Networks, 2005, pp. 223–245.

[11] S. Bansal, M. Baker, Observation-based Cooperation Enforcement in Ad hoc Networks, in: Proceedings of ACM/IEEE International *Conference* on Mobile Computing and Networking, 2004, pp. 325–355.

[12] Anker. Tal, Doley. Danny, Hod. Bracha, Cooperative and Reliable Packet Forwarding on Top of AODV, in: 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and wireless Networks, 2006, pp. 241–250.

[13] T. Sakthivel, R.M. Chandrasekaran, A Dummy Packet-Based Hybrid Security Framework for Mitigating Routing Misbehavior in Multi-Hop Wireless Networks, Wirel. Pers. Commun. 101 (3) (2018) 1581–1618.

[14] J. Sen, Security and Privacy Issues in Wireless Mesh Networks: a Survey, in: S. Khan, AS. Khan Pathan (Eds.), Wireless Networks and Security. Signals and Communication Technology, Springer, Berlin, Heidelberg, 2013.

[15] D. Das, K. Majumder, A. Dasgupta, Selfish node detection and low cost data transmission in MANET using game theory, Procedia Comput. Sci. 54 (2015) 92–101.

[16] Y. Taheri, H.G. Garakani, N. Mohammadzadeh, A game theory approach for malicious node detection in MANET, Int. J. Comput. Inf. Syst. Sci. Eng. 32 (3) (2016) 559–573.

[17] Y. Wang, A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad-Hoc Networks, Carleton University, Ottawa, Ontario, Canada, 2014.

[18] M. Bounouni, Medjkoune.L. Bouallouche, A Hybrid Stimulation Approach for Coping against the Malevolence and Selfishness in Mobile Ad hoc Network, J. Wirel. Person. Commun. 88 (2) (2016) 255–281.

[19] Adnan Ahmed, Kamalrulnizam Abu Baker, Muhammad Ibrahim Channa, Khalid Haseeb, Abdul Waheed Khan, A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks, Front. Comput. Sci. (2) (2015) 280–296.

[20] S. Sen, J.A. Clark, Intrusion Detection in Mobile Ad Hoc Networks, in: S. Misra, I. Woungang, S. Chandra Misra (Eds.), Guide to Wireless Ad Hoc Networks. Computer Communications and Networks, Springer, London, 2009, pp. 427–454.

[21] M. Janusz Kusyk, Uyar. Umit, Sahin. Cem Safak, Survey on evolutionary computation methods for cyber security of mobile ad hoc networks, J. Evolution. Intellig. 10 (3–4) (2018) 95–117.

[22] Basant Subba, Santosh Biswas, Sushanta Karmakar, A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks, Int. J. Wireless Inf. Netw. 25 (4) (2018) 399–421.

[23] Abderrahmane Baadache, Ali Belmehdi, Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks, J. Netw. Comput. Appl. 35 (3) (2012) 1130–1139.

[24] M. Mohanapriya, I. Krishnamurthi, Modified DSR protocol for detection and removal of selective black hole attack in MANET, Comput. Electr. Eng. 40 (2) (2014) 530–538.

[25] R.M. Sandhya, Pramod M.Murari, M.Mayannavar. Shanoor, S.G. Gollagi, Y.M. Naik, Internet Traffic Classification by Aggregating Correlated Naive Bayes Predictions, Int. J. Sci. Dev. Res. (IJSDR) (2017) 241–247.

[26] Yatin Chauhan, Jaikaran Singh, Mukesh Tiwari, Anubhuti Khare, Performance Evaluation of AODV based on black hole attack in ad hoc network, Glob. J. Res. Eng. Electric. Electron. Eng. 12 (2) (2012).

[27] E. Sivajothi, N. Vijayalakshmi, A. Swaminathan, P. Vivekanandan, An Overview of Route Discovery Mechanisms of Multicast Routing Protocols for MANETs, Int. J. Eng. Tech. (IJET) 5 (5) (2013) 3958–3966.

[28] Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamal, Security improvements Zone Routing Protocol in Mobile Ad Hoc Network, Int. J. Comp. Appl. Tech. Res. 3 (9) (2014) 536–540.

[29] L. Govindaraj, B. Sundan, A. Thangasamy, An Intrusion Detection and Prevention System for DDoS Attacks using a 2-Player Bayesian Game Theoretic Approach, in: 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021, pp. 319–324.

[30] A.; B. Thangasamy, B. Sundan, L. Govindaraj, Dynamic PHAD /AHAD Analysis for Network Intrusion Detection and Prevention System for Cloud Environment, in: 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021, pp. 273–279.

[31] Satish Ganapathy, P. Vijayakumar, Yogesh Palanichamy, Kannan. Arputharaj, An Intelligent CRF Based Feature Selection for Effective Intrusion Detection, Int. Arab J. Inform. Tech. 13 (2016) 44–50.

[32] Dukka KarunKumar Reddy, Himansu Sekhar Behera, Janmenjoy Nayak, Pandi Vijayakumar, Bighnaraj Naik, Pradeep Kumar Singh, Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities, Trans. Emerg. Telecommun. Tech. Vol. 32 (7) (2021) e4121.

[33] X. Li, M. Xu, P. Vijayakumar, N. Kumar, X... Liu, Detection of Low-Frequency and Multi-Stage Attacks in Industrial Internet of Things, IEEE Trans. Veh. Technol. 69 (8) (2020) 8820–8831.

[34] B. Bera, A.K. Das, M.S. Obaidat, P. Vijayakumar, K.F. Hsiao, Y. Park, AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE, IEEE Consum. Electron. Mag. 10 (5) (2021) 82–92.

[35] Ning Lu, Dan Li, Wenbo Shi, Pandi Vijayakumar, Francesco Piccialli, Victor Chang, An efficient combined deep neural network based malware detection framework in 5 G environment, Comput. Netw. Chem. Lab., Symp. 189 (2021).