International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2096
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Cyber-Attack Detection in Autonomous Vehicle Networks by Energy Aware Optimal Data Transmission with Game Fuzzy Q-Learning based Heuristic Routing Protocol

Waleed F. Faris
Professor,
International Islamic University Malaysia,
Kuala Lumpur- 53100, Malaysia
https://orcid.org/0000-0002-1219-8793

Abstract:
The automotive sector has seen a dramatic transition due to rapid technological advancement. Network connection has improved, enabling the transfer of the cars' technologies from being fully machine- to software-controlled. Controller area network (CAN) bus protocol manages network for autonomous vehicles. However, due to the intricacy of data and traffic patterns that facilitate unauthorised access to a can bus and many sorts of assaults, the autonomous vehicle network still has security flaws as well as vulnerabilities. This research proposes novel technique in cyber attack detection in autonomous vehicle networks enhanced data transmission based optimization and routing technique. Here the autonomous vehicle network optimal data transmission has been carried out using energy aware lagrangian multipliers based optimal data transmission. The cyber attack detection has been carried out using fuzzy q-learning based heuristic routing protocol. The experimental results has been carried out based on optimal data transmission and attack detection in terms of throughput of 95%, PDR of 94%, End-end delay of 46%, energy efficiency of 96%, network lifetime of 95%, attack detection rate of 88%.

Keywords: cyber-attack detection, autonomous vehicle networks, data transmission, optimization, heuristic routing protocol.

1. Introduction:

As a subset of intelligent transportation method, connected and autonomous vehicles (CAV) use a numerous hardware, such as electronic control units (ECUS) and sensors, software, like entertainment methods, decision-making units and data merged from various sources to perform driving tasks with changing degrees of automation. With these elements, CAVS may not only operate autonomously but also communicate with their environment to navigate and respond appropriately [1]. The sensors placed all over the vehicle body, which collect data from the surroundings to inform decisions, help the automation of CAVS. To navigate and respond appropriately, connectivity is achieved via interacting with other vehicles, infrastructures, and pedestrians on route. Many businesses are currently looking into and concentrating on CAVS research and development. An open source autonomous driving platform called apollo was recently launched by one of the major technology businesses in China, Baidu, with the goal of tackling the difficult problems of precise sensing as well as decision-making. Tesla unveiled its autopilot for driving assistance as well as summon system for parking assistance in the United States in 2015 and 2016, respectively [2]. The upgraded autopilot technology, which permits autonomous driving in some circumstances, such as on highways, is described in the most recent news on Tesla's official website. Google is a pioneer in connected and automated driving, as well. Its 2009-founded subsidiary Waymo has focused on the research as well as development of CAVsas well as has completed more than 2 million miles of road testing. Uber, a ride-hailing service, additionally tests its own cavs on open roads in Arizona [3]. Traditional automakers in Europe like Audi as well as Mercedes-Benz also reveal their initiatives regarding CAVs. Audi is tested their own autonomous vehicle "jack" for 550 kilometres on public roads. Mercedes-Benz began creating cavs in the 1980s; as of late, its s-class models have successfully undergone 100 km of road testing in Germany [4].

In order to make both immediate and long-term driving decisions, a fully autonomous car relies on sensor readings. The high-tech architecture of these autos improves communication between the sensors [5]. To improve their ability to manoeuvre autonomously, self-driving cars use sophisticated control panels. But there are dangers and hazards in the technological world, particularly aggressive hacker, bug, and virus attacks. To improve their dependability, accuracy, and other elements, self-driving cars have cutting-edge data encryption and protection. Many cutting-edge devices are integrated into automatic vehicles, improving navigation through route maps and radio frequency characteristics. Automatic cars still carry a significant danger of being attacked and have the potential to do so with any technology installed in them [6].

The contribution of this research is as follows:

1. To propose novel method in cyber attack detection in autonomous vehicle networks enhanced data transmission based optimization and routing technique
2. To design energy aware lagrangian multipliers based optimal data transmission for optimal data transmission
3. The cyber attack detection has been carried out using fuzzy q-learning based heuristic routing protocol.

2. Background study:

Driving automation, according to the SAE International, is when a technology can do all or a portion of dynamic driving tasks (DDT) constantly [7]. The sae j3061 standard defines DDT as having three separate levels, namely operational functions, tactical functions, and strategic functions. Possible CAV cyber-attacks are listed in [8]. It was determined that among the most dangerous cyber threats are GNSS spoofing and the introduction of bogus communications. Potential cyberattacks were divided into passive as well as active attacks in [9], which are the two main categories. While active attacks, such as modification and spoofing, are simple to identify but challenging to defend against because attackers can alter or fake the messages in the data transmission, passive attacks, such as eavesdropping and the release of information, are difficult to detect but simple to defend against. The authors of [10] noted that the present automotive safety standard, ISO26262, does not take security concerns into account in order to prevent both unintended and intentional attacks. There isn't yet a global standard for CAVs security or safety. For the development of CAVs, a systematic specification of attacks as well as methodologies for attack analysis are consequently particularly desirable. Other studies have examined targeted attacks against CAVs in order to suggest potential AI-based remedies, in addition to talks of prospective attacks on CAVs. The authors of [11] conducted a thorough study of the current ML based adversarial assaults against CAVs. As well as being separated into application layer, network layer, system level, privacy breaches, sensors assault, and so forth, the prospective attacks were also subdivided. The authors of [12] emphasised the critical role that intrusion detection plays in the creation of CAVs. In order to train in-vehicle network traffic data against threats and detect intrusion, work [13] uses an Inception-RESNET model. The results have been compared to a number of existing models, including decision tree algorithms, LSTM, NNs, SVM, NB approaches. To protect the can bus from attacks, the author in [14] created an intrusion detection system. The authors employed a hybrid method, specifically gradient descent momentum as well as adaptive gain, to classify attackers' message. DNN based intrusion detection was used in study [15] to monitor the can bus message frame. DBN function was DL model employed for the training procedure, and it has been demonstrated that this model's accuracy can reach 98 percent for the suggested system. To analyse network traffic for novel network packet patterns and compare them with patterns on IDS method, author in [16] constructed an ids system in can bus. It was noted that their system obtained great accuracy when compared to the conventional system. According to study [17], a distributed anomaly classification can be designed using a hierarchical temporal memory approach. According to the empirical findings, the model needs more time to detect attacks. In order to create adversarial assaults, a variety of ML as well as DL techniques have been used to predict incursions on can bus, including DNN [18], CNN, and ANNs. In 2015, a Jeep Cherokee was remotely compromised in order to increasealertness about cybersecurity of cars [19]. According to a recent study [20], as it is difficult to manufacture a vehicle with a security method that guards it against attacks, primary goal of research should not be to prevent attacks.

3. Proposed cyber attack detection in autonomous vehicle networks:

This section discuss novel technique incyber attack detection in autonomous vehicle networks enhanced data transmission based optimization and routing technique. Here the autonomous vehicle network optimal data transmission has been carried out using energy aware lagrangian multipliers based optimal data transmission. The cyber attack detection has been carried out using fuzzy q-learning based heuristic routing protocol. It's also possible for attacks to target AVS radio communication. In order to corrupt the packet during data transmission before it can be received, the attacker uses a diminishing signal-to-noise ratio or significant latency between the transmitter and receiver. The attacker can use this technique to significantly impede communication between the sender and the receiver. Road congestion reduces productivity and costs money in wasted time and fuel. AVs collaboration improves traffic flow. Smart vehicles are projected to reduce the number of accidents and fatalities related to road safety. The subject of most recent study is autonomous vehicle localisation technologies. These autonomous systems take input that is malevolent into account. This is incorrect from the standpoint of security by design, as an AVs decisions are only as good as what its sensors can detect. A harmful situation may result from a poor observation. Figure 1 depicts the sensor network based on AV.

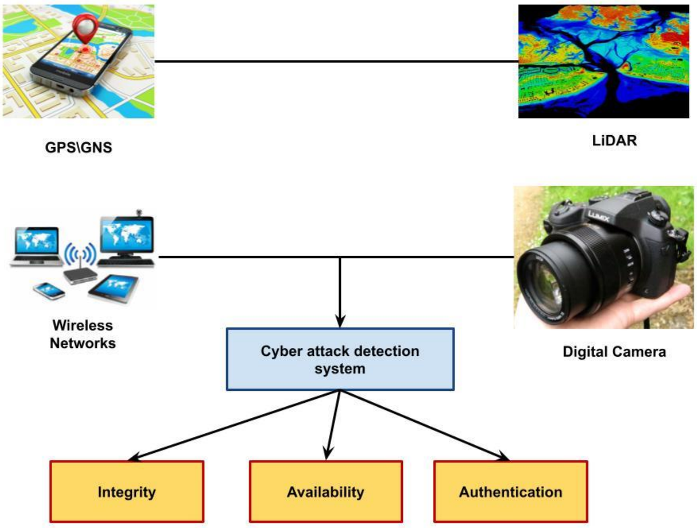


Figure-1 AV based sensor network

Energy aware lagrangian multipliers based optimal data transmission (EALM_ODT):

We provide an energy consumption method for sending a packet with transmit power pt over a distance d. Energy use in SGNs primarily happens for the following reasons: (i) how much power is needed to turn on transmitter as well as receiver, (ii) energy needed for transmission and reception processing, (iii) the power needed to send packets, (iv) the power necessary for acknowledgment (ack) transmission, and (v) the amount of energy used in sleep or idle state. Let ee represent the amount of energy needed to process one data bit in the transmitter and one in the receiver.The formula for calculating value of ee is provided as ee = ptx r, where ptx denotes processing power both at the transmitter and the receiver and r = rbrc denotes bit rate with coding rate rc.As a result, eproc = 2eelnx is presented as the energy consumption for processing packet at transmitter and receiver. The formula etx = ptlnx r indicates how much energy is used to transmit each packet. By a result, the total energy needed to send a packet of length l over a distance of d is represented as eq (1)

$$E = 2E_eLN_x + P_t\frac{LN_x}{R} \qquad (1)$$

A model called eq(2) can be used to calculate the overall energy needed to send a packet of length l over a distance d.

$$E = (a + bP_t)\exp\,(c/P_t)$$
$$a = 2E_eL$$
$$b = L/R \qquad (2)$$

Energy consumption e n,k is represented as per the energy model in (3).

$$E'_{n,k} = \left(a_k + b_kP'_{n,k}\right)\exp\left(c'_{n,k}/P'_{n,k}\right) \qquad (3)$$

Where, by swapping out l and d for lk + h and dn,bs, values of specificationsak, bk, and c n,k may be determined. The energy consumption, e n,i,k, is also specified as eq (4)

$$E''_{n,i,k} = \left(a_k + b_kP''_{n,i,k}\right)\exp\left(c''_{n,i,k}/P''_{n,i,k}\right) \qquad (4)$$

Where, by changing l and d to lk + h and dn,i, from (4), value of specification c n,i,k may be derived. The entire amount of energy used to deliver the data traffic directly eq (5)

$$E_{sm2bs} = \sum_{n\in\mathcal{N}} x_n\left(\sum_{k\in\mathcal{K}} E'_{n,k}\right) \qquad (5)$$

Similar to this, the overall energy used to transport the data stream by eq (6)

$$E_{sm2ag} = \sum_{n\in\mathcal{N},i\in\mathcal{I}} y_{n,i}\left(\sum_{k\in\mathcal{K}} E''_{n,i,k}\right) \qquad (6)$$

The total amount of energy used to send the data packets through eq (7)

$$E_{sm} = E_{sm2bs} + E_{sm2ag} \qquad (7)$$

If the entropy fulfils $e^{-H_i(t'} \sim 1 - H'_i(t)$, the cross-layer optimization model is roughly convex, and we build the lagrangian issue by reducing the restrictions as shown in eq (8)

$$\begin{aligned} & L(x_i(t), f_i'(t), I_i'(t), E_i(t), \lambda_i, \alpha_i, \beta_i, \gamma_i) \\ & = \sum_{i=1}^{N} U(x_i(t), f_i'(t), I_i'(t), E_i(t)) \\ & +\lambda_i(t)\left(x_i(t) + \sum_{j\in Y_{(i)}} r_{ij}(t) - \sum_{j\in\mathbb{T}_{(i)}} r_{ij}(t)\right) \\ & +\alpha_i(t)\left(f_i'(t) - x_i(t) - \sum_{j\in Y(t)} r_{ji}(t)\right) + \\ & \beta_i(t)\left(\mathrm{P}_r^t\left(H_i^j(t)\right) - e^{-H_i(t)}\right) \qquad (8) \\ & +\gamma_i(t)\left(\bar{E}(t) - \sum_{i=1}^{N} E_i(t)\right) \quad . \end{aligned}$$

Where li(t), ai(t), bi(t), and gi(t) are conservation-constrained lagrangian multipliers. We employ distributed sub-gradient approach because l(.) is only piecewise differentiable. Concatenated into m types of packets will be complete amount of data traffic that has been gathered at this traffic. To perform the concatenation operation at the ag I let quantity of packets of type m m increase to nm,i. Let di,bs represent the separation between ag I and bs. Indicate by em,i amount of energy used to transport a concatenated type-M data packet from ag I to bs. Let pm,i represent transmit power needed to transfer a type M data packet from ag I to bs. Amount of energy consumed is expressed as eq. (9) (em,i).

$$E_{m,i} = \left(a'_m + b'_m P_{m,i}\right)\exp\left(c'_{m,i}/P_{m,i}\right) \qquad (9)$$

Where, by swapping out l and d for l m + h and di,bs, specifications a m, b m, and c m,iare derived. The amount of energy used to transmit the combined data traffic from ags to bs is indicated as eq (10)

$$E_{ag} = \sum_{m\in\mathcal{M},i\in\mathcal{I}} N_{m,i} E_{m,i} \qquad (10)$$

Furthermore, let em,i(min) be least value of function em,I by eq. (11) for a assumed m ∈ m and i∈i.

$$\begin{aligned} & \min_{\mathbf{x},\mathbf{y},\mathbf{N}'} \sum_{n\in\mathcal{N}} x_n\left(\sum_{k\in\mathcal{K}} E'_{n,k}(\min)\right) \\ & +\sum_{n\in\mathcal{N},i\in\mathcal{I}} y_{n,i}\left(\sum_{k\in\mathcal{K}} E''_{n,i,k}(\min)\right) \\ & + \sum_{m\in\mathcal{M},i\in\mathcal{I}} N_{m,i} E_{m,i}(\min) \\ & x_n + \sum_{i\in\mathcal{I}} y_{n,i} = 1 \quad \forall n \in \mathcal{N} \\ & \qquad (11) \\ & \sum_{n\in\mathcal{N}} y_{n,i}\left(\sum_{k\in\mathcal{K}} L_k\right) \le \sum_{m\in\mathcal{M}} N_{m,i} L'_m \quad \forall i \in \mathcal{I} \\ & \mathbf{x}, \mathbf{y} \in \{0,1\}, \mathbf{N}' \in \mathbb{Z}, 0 \preceq \mathbf{N}' \end{aligned}$$

Our objective is rate maximisation under circumstances when eq. (12) provides a sufficient level of connection capacity, routing, and power allocation.

$$P_1 \max x_i(t) \qquad (12)$$

by using l's derivative (.) Using xi(t) and li(t), we arrive to the following equational solution (13),

$$\frac{\partial L}{\partial x_i}(t) = \frac{\partial \sum_{i=1}^{N} U_i}{\partial x_i}(t) + \lambda_i(t) - \alpha_i(t)$$

$$\frac{\partial L}{\partial \lambda_i}(t) = x_i(t) + \sum_{j\in Y_{(i)}} r_{ji}(t) - \sum_{j\in T_{(i)}} r_{ij}(t) \qquad (13)$$

Since p1 is roughly convex issue, eq. (14) is used to resolve it

$$x_i(t+1) = \left[x_i(t) + \varepsilon\frac{\partial L}{\partial x_i}(t)\right]^+$$

$$\lambda_i(t+1) = \left[\lambda_i(t) - \varepsilon\frac{\partial L}{\partial \lambda_i}(t)\right]^+ \qquad (14)$$

where $[x]^+ = \max(0, x)$ and ε is the step size.

For the maximisation of link capacity f l I (t), P2 is similarly roughly convex, and the method of implementation is similar to p1 by eq (15)

$$P_2 \quad \max f_i'(t) \qquad (15)$$

The answers are derived, respectively, as eq. (16), by taking derivative of $L(\cdot)$ with $f_i^l(t)$ and $\alpha_i(t)$,

$$\frac{\partial L}{\partial f_i'}(t) = \frac{\partial \sum_{i=1}^{N} U_i}{\partial f_i^l}(t) + \alpha_i(t)$$

$$\frac{\partial L}{\partial \alpha_i}(t) = f_i^l(t) - x_i(t) - \sum_{j\in Y(i)} r_{ji}(t) \qquad (16)$$

Updates to the link capacity and lagrangian multiplier is made as eq (17)

$$f_i^l(t+1) = \left[f_i^l(t) - \varepsilon\frac{\partial L}{\partial f_i^l}(t)\right]^+$$

$$\alpha_i(t+1) = \left[\alpha_i(t) - \varepsilon\frac{\partial L}{\partial \alpha_i}(t)\right]^+ \qquad (17)$$

One of the most crucial problems, according to eq. (18), is trade-off between power as well as transmission efficiency

$$P_3 \quad \min E_i'(t) \qquad (18)$$

Taking derivative of $L(\cdot)$ with $E_i^l(t)$ and $\gamma_i(t)$ by eq. (19)

$$\frac{\partial L}{\partial E_i}(t) = \frac{\partial \sum_{i=1}^{N} U_i}{\partial E_i}(t) - \gamma_i(t) \qquad (19)$$

By eq. (20) it is demonstrated that pi(t) and gi(t) may be obtained using the same method

$$E_i(t+1) = \left[E_i(t) - \varepsilon\frac{\partial L}{\partial E_i}(t)\right]$$

$$\gamma_i(t+1) = \left[\gamma_i(t) - \varepsilon\frac{\partial L}{\partial \gamma_i}(t)\right]^+ \qquad (20)$$

The decision variables of sms, x and y, as well as concatenation variables, n, can be used to separate the lagrangian function. As a result, eq. (21) can be used to decompose the dual function.

$$D(\gamma) = D_{sm}(\gamma) + D_{agg}(\gamma)$$

$$D_{agg}(\gamma) = \min_{\mathbf{N}'} \left\{ \sum_{m \in \mathcal{M}} N_m [E_m(\mathrm{m} \quad) - \gamma L'_m] \mid \begin{matrix} \mathbf{N}' \in \mathbb{Z} \\ 0 \le \mathbf{N}' \end{matrix} \right\} \tag{21}$$

Solution of sub-issuedsm(γ) is quite simple. For a sm n ∈ni, xn = 1 and yn = 0 $E'_n(\mathrm{m} \quad) \le E''_n(\mathrm{m} \quad) + \gamma L^t$

Lagrange multiplier γ thus illustrates advantages of aggregation. The likelihood that a sm will select ag I for data packet transmission grows as value of γ rises. Answer to subproblem dagg(γ) is likewise straightforward.

Algorithm of EALM_ODT:

```
Require:
N
V(I,j),I,j=1,2,…….N
S(a,b)
Neighbor vi{}
r
Ensure:
List GH{i|i=1,……….$N_{opy-CH}$}
Assert List CH{}=NULL
For i=1 to N do
Evaluate candidate value of node $v_i$ as a CH
    $CH_{candidate-i} = \alpha.\left(\frac{E_{Remain-i}}{E_{Initial}}\right) + \beta.\left(\frac{Deg_{max}}{Deg_i}\right) + \gamma.(\frac{Dis_{i-sink}}{Dis_{max-sink}})$
End for
For i=1 to N do
N=+1
For j=i+1 to N do
If $n \neq N_{opt-CH}$then
If $CR < 90\%$ then
take next node $v_j$
End if
End if
End for
End for
```

Fuzzy q-learning based heuristic routing protocol:

This research enhanced the self-learning capability of the detector agent by optimising fuzzy logic controller (FLC) via q-learning method to detect type of attack a node may experience in future. By using corresponding membership functions, the fuzzification process transforms variables x∈ x, where x is set of potential input variables, into fuzzy linguistic variables. Inference engine (ie) converts fuzzy sets from input and output to q-values. q-value and fuzzy rules used to update its eligibility. A crisp value to adopt an action in terms of action policy is computed by defuzzification. By simply discretizing the action value policy, q-learning can be modified to handle continuous state and action spaces. The suggested fuzzy q-learning (FQL) architecture is represented in Figure 2.

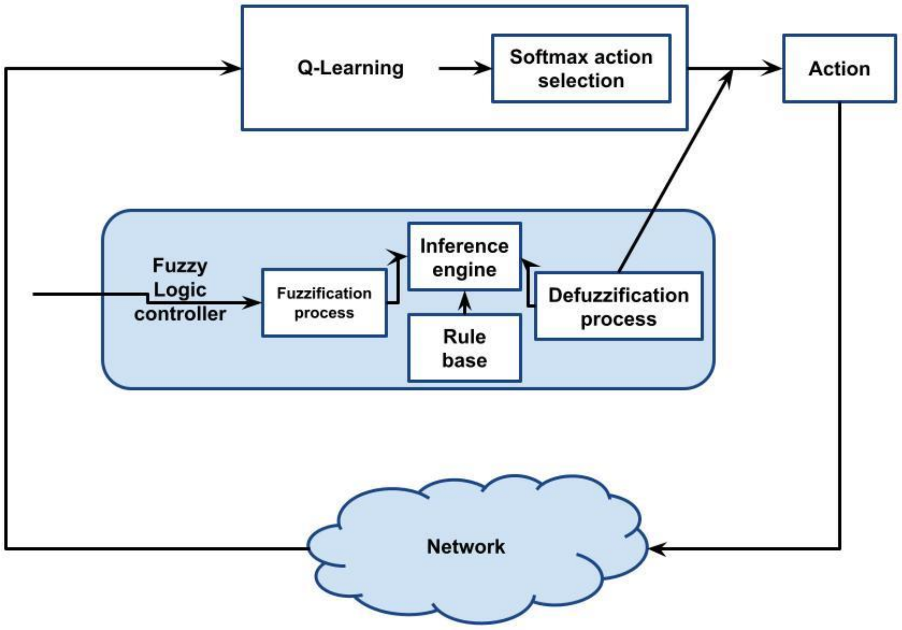


Figure-2 block diagram of fuzzy q-learning architecture

In decision-making procedures where the system under control, but also the goals and/or restrictions, can be fuzzy q-learning extends q-learning technique. "The weight of object a must not be substantially heavier than w," where ui is a given weight, is an illustration of a fuzzy constraint. Similarly, "the robot must be near door k" is an illustration of a hazy goal. The value of executing action an in state z is estimated by q-learning method as q(z, a). Similar to this, when using fq-learning process, we keep an evaluatefq(z, a) for performing action an in state z, where actions may be subject to fuzzy restrictions, and continuing the best course of action until a new state has been attained. According to equation (22): "The value of a state is the value of the state's best state action pair."

$$V(x) = Max_a FQ(x,a) \qquad (22)$$

The definition of the actual q value of an inferred action an in state x in eqn. (23).

$$Q(x,a) = \frac{\sum_{i=1}^{k} \alpha_i(x) q_i(c_i^*)}{\sum_{i=1}^{k} \alpha_i(x)} \qquad (23)$$

Let xt, xt+1 represent the system's present and future states.Following equation (24) can be used to determine error of calculation for a q function:

$$\Delta Q = r + \gamma Q(x_{t+1}, a\,*) - Q(x_t, a) \qquad (24)$$

Where a represents "the best" course of action in state xt+1. It is made up of the conclusions for each rule with highest q value. Gradient descent approach yields a formula for updating q lookup vectors that has the shape of eq. (25):

$$\Delta q_i(c_j) := \beta \Delta Q \frac{\alpha_i(x)}{\sum_{i=1}^{k} \alpha_i(x)} \qquad (25)$$

Attack data source: According to the vulnerability scanning information, the attack data source is described as a 5-tuple ads={pt,dp,tr,bs,co}, where ptis type of protocol (tcp=1, udp=2); dpis destination port.

Before using fuzzy decision procedures with rule base, every input variable's sharp value must first be fuzzified into linguistic values. Values between 0 and 1, which represent an element's level of membership in a particular set, are given the characteristic function of a fuzzy set.

The heuristic function established by packet Mk and node I is shown in equation (26). As a result, there are two components to the function in (1). The second portion heuristically calculates the anticipated needed hop count between current node I and destination node d by eq. First part reflects actual passed hop count of message Mk (26),

$$\mathcal{H}(i,k) = hop(k) + h(i,d) \qquad (26)$$

Heuristic function h(i, d) is displayed precisely in equation (27). Calculated hop count of path between nodesi and d is represented by Path[$i \longrightarrow d$], which differs from total number of paths between nodesi and d. Consequently, h(i, d) actually refers to average number of hops taken by all pathways between iand d. As a heuristic metric for our routing, we use this value.

$$h(i,d) = \frac{\sum_{c=1}^{c=m} path_c[i{\rightarrow}d]}{m} \qquad (27)$$

By implementing a special operation on matrix⊙, which is described as follows eq. (28), we are able to determine the heuristic value.Consider that M and N are both $n{\times}n$matrices and that $O{=}M{\odot}N$, one has for any member oi of the matrix O

$$o_{i,j} = \frac{\sum_{k=1}^{k=n}(m_{i,k} + n_{k,j})}{w}$$

$$w = |\{c|c = m_{i,k} + n_{k,j}, c > 0\}| \qquad (28)$$

This algorithm's input is matrix A, which is kept up to date by node i. We finally obtain all heuristic values $h(i,\ *)$ for every message held by node I by running this procedure, where ∗denotes the id of any potential destination for a packet. As seen in line 1, outer loop cycles through set of every packet belonging to node i. We initialise the three crucial variables h, c, and M in lines 2-4. Each time the inner loop iterates, these three variables are updated recursively. The total number of pathways in each iteration are tallied using the local variable c. In each iteration of the while loop, M will be multiplied by A from its initial state of λ. The node ids for Mk's current node and destination node are obtained on lines 5 and 6, respectively. If there is no h-hop path connecting nodes I and d, the inner loop does not end until element mi of matrix M is zero. As stated in line 13, h(i, d) is then set to be average number of hops between current node I and destination node d.

Algorithm

```
Need: Matrix $A$ of node i
Ensure: $f(i,*)$
local variables: $i_2 h_1, c_{r\ d}$
(1) for $M_k \in$ imessages do
(2) $h \leftarrow 0$
(3) $c \leftarrow 0$
(4) $M \leftarrow \Lambda$
(5) i← getHostIDO
(6) $d \leftarrow M_k$ getDestinationID()
(7) repeat
(8)    $M \leftarrow M \odot A \quad m_{i,d} = m_{1,5} = \frac{[0+0+(1+2)+(3+7)+0]}{2} = 6.5,$
(10) $c \leftarrow c + 1$
(ii) until $m_{idi} = 0 \quad h = 5 + 6.5 = 11.5,$
(12) $h(i,d) = h/c$
(13) end for
(14) return $h(i,*)$
```

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2096
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Consider that node I is node currently executing heuristic method and that message Mk was produced at source node s and is anticipated to arrive at destination node d. There have been a total of 6 hops for the packet Mk from node s to node I therefore hop(k) = 6. We have by eq. (29) for the inner while loop's initial iteration,

$$M = A \bigcirc A = \begin{pmatrix} 0 & 2 & 1 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad (29)$$

Where we have by eq. (30)

$$m_{i,d} = m_{1,5} = 5$$
$$h = 0 + 5 = 5$$
$$c = 0 + 1 = 1 \qquad (30)$$

For second iteration, we have by eq. (31)

$$M = A \bigcirc A = \begin{pmatrix} 0 & 0 & 0 & 0 & 6.5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad (31)$$

Where we have by eq. (32)

$$m_{i,d} = m_{1,5} = \frac{[0 + 0 + (1 + 2) + (3 + 7) + 0}{2} = 6.5$$
$$\text{H=5+6.5=11.5}$$
$$\text{C=1+1=2} \qquad (32)$$

Due to the fact that the element mi, = m1,5 = 0, and ultimately the presence of by eq (33), the while loop terminates before the third iteration

$$h(i, d) = \frac{h}{c} = \frac{11.5}{2} \approx 5.75 \qquad (33)$$

Keep in mind that the h(i, d) number calculated above is a rough estimate of its definition. Using (33), we get at the average hop count value of 6, which is very similar to our calculation's result of 5.75. It is fair to streamline the calculation procedure using such a method because the goal is to estimate the required hop count rather than to determine the exact average hop count value.

Algorithm of FQL-HRP:

```
Input: NTable, H table, L table, D
Output: The next hop (nexthop)
        $cost_{min} = d_{n1} \rightarrow D$
Nexthop=$n_1$
For each neighbor$n_1$ in N table do
Flag=false
For each record RL in L table do
If RLj.neighbor==ni and
RLj.destination ==D then
Flag=true;
Cost=RLj.cost
End
End
Of flag==false then
Add a new record RL new;
RL new.destination =D
RLnew.cost=$d_{n1} \rightarrow D$
Cost=RLnew.cost
End
If $cost < cost_{min}$then
        $cost_{min} = cost;$
Nexthop=n;
End
End
Flag=false
Hvalue=$d_x \rightarrow nexthop + cost_{min}$
For each record$RH_i$ in H table do
If $RH_i$ destination == D the
Flag=true;
        $RH_i.hvalue = hvalue$
Break
End
End
If flag== false then
Add a new record RH new
RH new.destination =D;
RH new.hvalue=hvalue;
End
Send broadcast of hvalue for D to its neighbor s;
```

4. Experimentation and results:

On a machine with a 3.70 GHz Intel Core i3 processor and a 64-bit version of Windows, the testing were conducted. Weka is a piece of free software for data mining that was created by the University of Waikato. It is utilized extensively in business as well as academia to do analysis and create MLmethods.

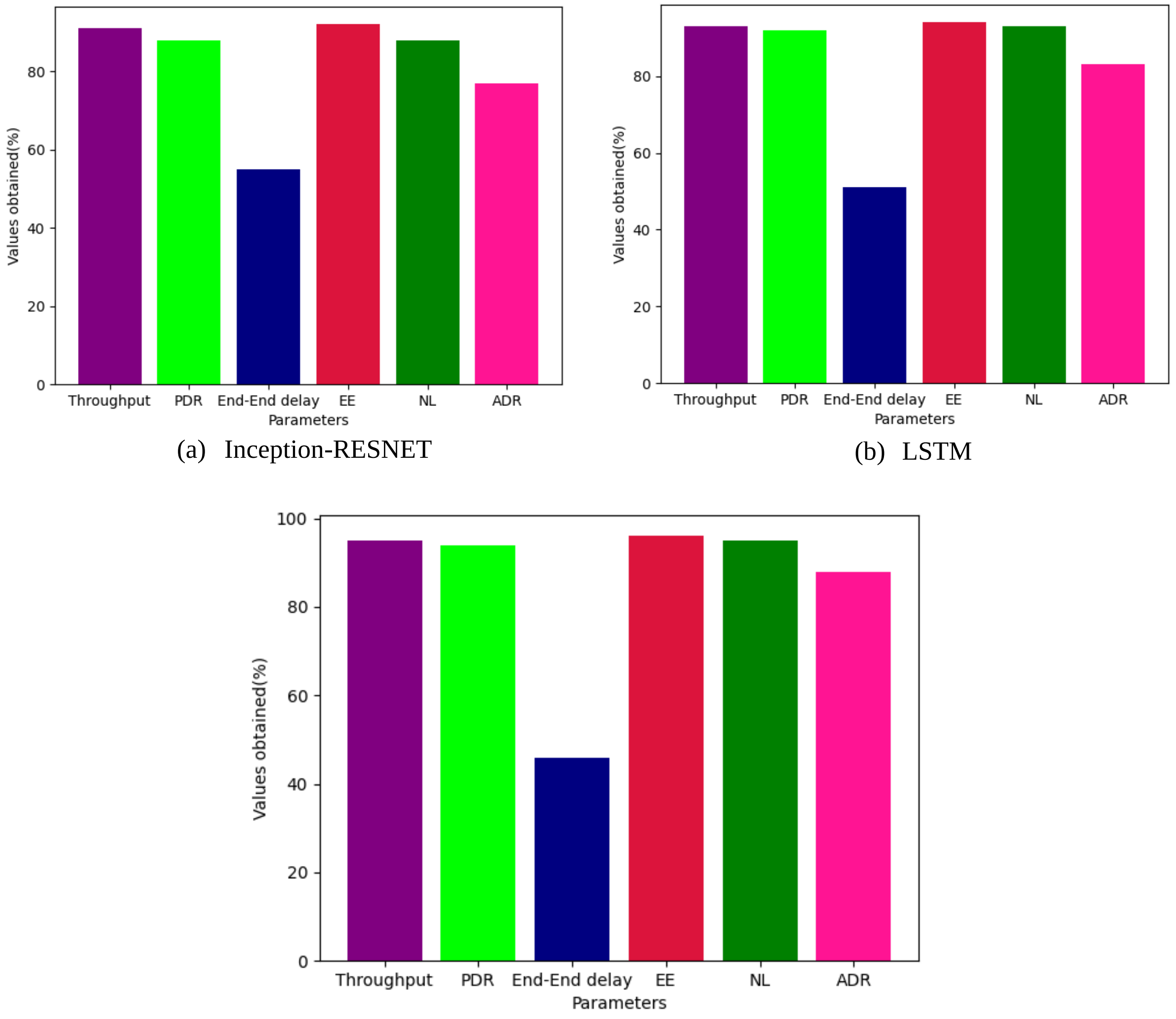
Dataset description:

The CAV dataset was compiled from actual can traffic data, which also included innocuous packets and assaults like spoofing, flooding, and replaying. The dataset was created by creating an obd-ii port for can traffic from a genuine CAV and injecting several forms of attack messages into the transferring messages. The open automobile testbed and network experiments (octane) with can packet generator were utilised. CAV traffic took 30 to 40 minutes, and the intrusions were injected every 3 to 5 seconds.

With more than 4 million data records, the KDD99 data collection is too large to be processed by personal computers.The training data set, which contained 10% of the kdd99 data set, was employed in this study. A new data collection, known as cav-kdd, that was compatible with the new CAV cyber security architecture was created after duplicates and irrelevant attack types were eliminated.

Table-1 Comparative analysis for CAV dataset between proposed and existing technique

Parameters	**Inception-RESNET**	**LSTM**	**EALM_ODT_ FQL-HRP**
Throughput	91	93	95
Packet Delivery ratio	88	92	94
End-End delay	55	51	46
Energy efficiency	92	94	96
Network lifetime	88	93	95
Attack detection rate	77	83	88



(a) Inception-RESNET

(b) LSTM

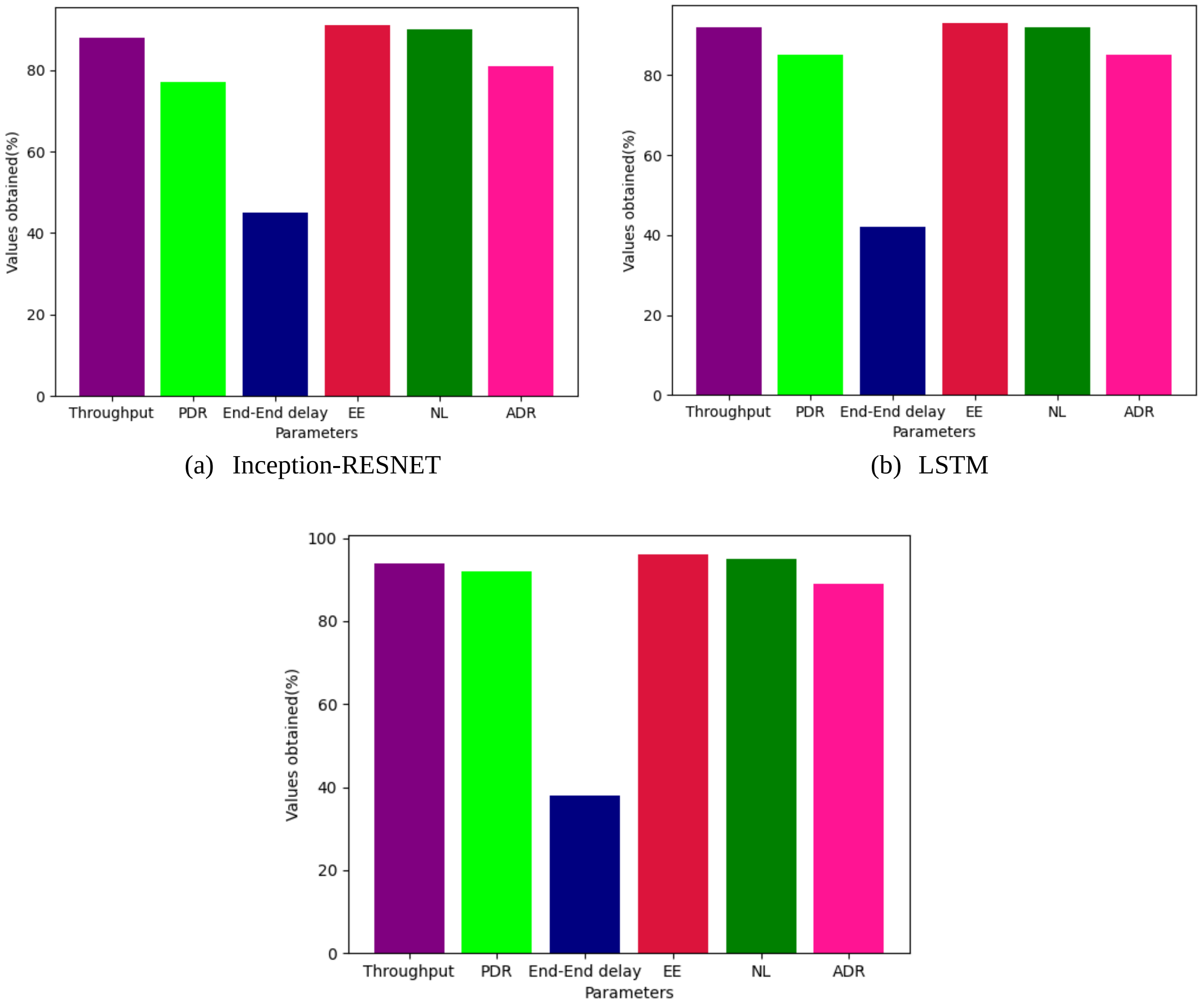
(c) EALM_ODT_ FQL-HRP

Figure-3 Comparative analysis for CAV dataset (a) Inception-RESNET, (b) LSTM, (c) EALM_ODT_ FQL-HRP

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 3
DOI: https://doi.org/10.17762/ijfrcsce.v8i3.2096
***Article Received**: 10 June 2022 **Revised**: 20 August 2022 **Accepted**: 25 August 2022 **Publication**: 15 September 2022*

Table-2 Comparative analysis for KDD99 dataset between proposed and existing technique

Parameters	**Inception-RESNET**	**LSTM**	**EALM_ODT_ FQL-HRP**
Throughput	88	92	94
Packet Delivery ratio	77	85	92
End-End delay	45	42	38
Energy efficiency	91	93	96
Network lifetime	90	92	95
Attack detection rate	81	85	89



(a) Inception-RESNET

(b) LSTM

(c) EALM_ODT_ FQL-HRP

Figure-4 Comparative analysis for KDD99 dataset (a) Inception-RESNET, (b) LSTM, (c) EALM_ODT_ FQL-HRP

The above table- 1 and 2 shows comparative analysis for proposed and existing technique for CAV and KDD99 datasets. Parametric analysis has been carried out in terms of throughput, PDR, End-end delay, energy efficiency, network lifetime, attack detection rate. PDR can be evaluated by dividing total number of data packets that have reached their destinations by the total number of packets that have been delivered from sources. In other words, PDR is proportion of packets delivered from source to those received at destination. When store-and-forward packet switches are employed, the formula for end-to-end delay for sending a single packet over N connections, each with a transmission rate of R, is d = N*L/R. Since the lifetime of each sensor node determines how long a wireless sensor network will last, energy efficiency is primary criterion for designing routing protocols for these networks. A routing protocol may also be data-centric. An essential performance parameter for WSNs is network lifespan, which is calculated as the period of time until the first sensor's energy runs out. In conventional WSNs, every sensor node is set up to transmit data collected to the sink via multihop communication. For CAV dataset, throughput of 95%, PDR of 94%, End-end delay of 46%, energy efficiency of 96%, network lifetime of 95%, attack detection rate of 88%, Inception-RESNET attained throughput of 91%, PDR of 88%, End-end delay of 55%, energy efficiency of 92%, network lifetime of 88%, attack detection rate of 77%, LSTM attained throughput of 93%, PDR of 92%, End-end delay of 51%, energy efficiency of 94%, network lifetime of 93%, attack detection rate of 83%. The proposed EALM_ODT_ FQL-HRP attained throughput of 94%, PDR of 92%, End-end delay of 38%, energy efficiency of 96%, network lifetime of 95%, attack detection rate of 89%, Inception-RESNET attained throughput of 88%, PDR of 77%, End-end delay of 45%, energy efficiency of 91%, network lifetime of 90%, attack detection rate of 81%, LSTM attained throughput of 92%, PDR of 85%, End-end delay of 42%, energy efficiency of 93%, network lifetime of 92%, attack detection rate of 85% for KDD99 dataset as shown in figure 3 (a)- (c), figure 4 (a)- (c).

5. Conclusion and discussion

In this research the proposed frameworks has been designed for cyber attack detection in autonomous vehicle networks. Here the optimal data transmission has been carried out using energy aware lagrangian multipliers based optimal data transmission. The cyber attack detection has been carried out using fuzzy q-learning based heuristic routing protocol. Experimental analysis has been carried out for various cyber attack dataset in terms of throughput, PDR, End-end delay, energy efficiency, network lifetime, attack detection rate. The proposed technique attained throughput of 95%, PDR of 94%, End-end delay of 46%, energy efficiency of 96%, network lifetime of 95%, attack detection rate of 88%. Last but not least, the suggested technique ensured secure data transfers between the greatest number of cars possible in the IoV environments. Future study will expand on this research to include residual node detection and other flooding attack consequences in the MANET environment mitigation.

Reference:

[1]. He, Q., Meng, X., & Qu, R. (2020). Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles. *Journal of advanced transportation*, *2020*.

[2]. Li, X. H., Hong, S. H., & Fang, K. L. (2009, September). A heuristic routing protocol for wireless sensor networks in home automation. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 1-8). IEEE.

[3]. Li, C., Wang, J., & Li, M. (2016). Data transmission optimization algorithm for network utility maximization in wireless sensor networks. *International Journal of Distributed Sensor Networks*, *12*(9), 1550147716670646.

[4]. Uddin, F. (2017). Energy-aware optimal data aggregation in smart grid wireless communication networks. *IEEE transactions on green communications and networking*, *1*(3), 358-371.

[5]. Lihua, L. (2022). Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods. *Wireless Communications and Mobile Computing*, *2022*.

[6]. Mahapatra, S. N., Singh, B. K., & Kumar, V. (2022). Secure energy aware routing protocol for trust management using enhanced Dempster Shafer evidence model in multi-hop UWAN. *Wireless Networks*, 1-18.

[7]. Ren, X., Vashisht, S., Aujla, G. S., & Zhang, P. (2022). Drone-edge coalesce for energy-aware and sustainable service delivery for smart city applications. *Sustainable Cities and Society*, *77*, 103505.

[8]. Kumar, R., Tripathi, S., & Agrawal, R. (2022). Trust-based energy-aware routing using GEOSR protocol for Ad-Hoc sensor networks. *Wireless Networks*, 1-24.

[9]. Nandi, M., & Anusha, K. (2021). An Optimized and Hybrid Energy Aware Routing Model for Effective Detection of Flooding Attacks in a Manet Environment. *Wireless Personal Communications*, 1-19.

[10]. Khan, I. U., Hassan, M. A., Alshehri, M. D., Ikram, M. A., Alyamani, H. J., Alturki, R., & Hoang, V. T. (2021). Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing. *Journal of Healthcare Engineering*, *2021*.

[11]. Geetha, B. T., Kumar, P. S., Bama, B. S., Neelakandan, S., Dutta, C., & Babu, D. V. (2022). Green energy aware and cluster based communication for future load prediction in IoT. *Sustainable Energy Technologies and Assessments*, *52*, 102244.

[12]. Islam, M. J., Rahman, A., Kabir, S., Karim, M. R., Acharjee, U. K., Nasir, M. K., ... & Wu, S. (2021). Blockchain-SDN-Based Energy-Aware and Distributed Secure Architecture for IoT in Smart Cities. *IEEE Internet of Things Journal*, *9*(5), 3850-3864.

[13]. Norouzi Shad, M., Maadani, M., &Nesari Moghadam, M. (2021). GAPSO-SVM: an IDSS-based energy-aware

clustering routing algorithm for IoT perception layer. *Wireless Personal Communications*, 1-20.

[14]. Aloqaily, M., Al Ridhawi, I., &Guizani, M. (2021). Energy-aware blockchain and federated learning-supported vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*.

[15]. Pérez, S., Arroba, P., & Moya, J. M. (2021). Energy-conscious optimization of Edge Computing through Deep Reinforcement Learning and two-phase immersion cooling. *Future Generation Computer Systems*, *125*, 891-907.

[16]. Lakshmanna, K., Subramani, N., Alotaibi, Y., Alghamdi, S., Khalafand, O. I., & Nanda, A. K. (2022). Improved Metaheuristic-Driven Energy-Aware Cluster-Based Routing Scheme for IoT-Assisted Wireless Sensor Networks. *Sustainability*, *14*(13), 7712.

[17]. Li, X. R., & Jiang, H. (2021). Energy-Aware Healthcare System for Wireless Body Region Networks in IoT Environment Using the Whale Optimization Algorithm. *Wireless Personal Communications*, 1-17.

[18]. Sadrishojaei, M., Jafari Navimipour, N., Reshadi, M., Hosseinzadeh, M., &Unal, M. (2022). An energy-aware clustering method in the IoT using a swarm-based algorithm. *Wireless Networks*, *28*(1), 125-136.

[19]. Ali, E. S., Hasan, M. K., Hassan, R., Saeed, R. A., Hassan, M. B., Islam, S., ... &Bevinakoppa, S. (2021). Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. *Security and Communication Networks*, *2021*.

[20]. Li, L., Qiu, Y., & Xu, J. (2022, April). A K-Means Clustered Routing Algorithm with Location and Energy Awareness for Underwater Wireless Sensor Networks. In *Photonics* (Vol. 9, No. 5, p. 282). MDPI.