Sustainable Computing: Informatics and Systems 23 (2019) 13–20

Contents lists available at ScienceDirect

Sustainable Computing: Informatics and Systems

journal homepage: www.elsevier.com/locate/suscom

DDoS attack detection: A key enabler for sustainable communication in internet of vehicles

Hafiz Husnain Raza Sherazi[a,*], Razi Iqbal[b], Farooq Ahmad[c], Zuhaib Ashfaq Khan[d], Muhammad Hasanain Chaudary[c]

[a] Department of Electrical and Information Engineering, Politecnico di Bari, Bari 70125, Italy
[b] College of Computer Information Technology, American University in the Emirates, Dubai International Academic City, Dubai, 503000, United Arab Emirates
[c] Department of Computer Science, COMSATS Institute of Information Technology, Lahore, 54000, Pakistan
[d] Deparment of Electrical Engineering, COMSATS University Islamabad, Attock Campus, Kamra Road, Attock, 43600, Pakistan

ARTICLE INFO

Article history:
Received 30 January 2019
Accepted 16 May 2019
Available online 25 May 2019

Keywords:
Sustainable communciation
Internet of vehicles
Intrusion prevention system
Machine learning
Fuzzy logic

ABSTRACT

Privacy and trustworthiness are the key apprehensions for the users of Internet of Vehicle (IoV) services. Having multiple components involved in the communication (i.e., sensors, vehicles, humans, and infrastructures), the IoV platforms are exposed to a range of attacks. This manuscript will focus on Distributed Denial of Service (DDOS) attacks by adding the design of an Intrusion Detection Systems (IDS) tailored to IoV systems. Moreover, Artificial Intelligence (AI) and Machine Learning (ML) techniques will be investigated that can help in making refined defense architecture for countering DDOS attacks in IoV networks. Furthermore, a fuzzy logic and Q-learning based proposed solution is tested through simulations which argues about the usefulness of the proposed approach in comparison with conventional techniques.

1. Introduction

The Internet of Things (IoT) is mainly based on smart devices connected together in a collaborative manner and interacting with the surrounding environment [1]. Internet of Vehicles (IoV) represents a specific use-case of IoT where information is shared between vehicles and the surrounding objects such as infrastructure, traffic lights, and pedestrian [2]. The IoV data generated by vehicles can be categorized into two parts: on-board data and on-road data. On-board data is referred to as the data used to monitor vehicle status like brake, velocity, and engine parameters. On-road data refers to the events data happening on road (e.g., inter-vehicle distance, blind point, pilot camera video, and traffic lights) [2].

Security in vehicular communication can be a major concern. With overwhelming number of vehicles on the road, and ever-changing relationship between the vehicles and vehicular communications are prone to become extremely complex. For the guarded environments such as 6LoWPAN networks, Routing Protocol for Low Power and Lossy Network (RPL) is conventionally employed. It is challenging to provide security in 6LoWPANs that are connected to IPv6/RPL because RPL does not work in the similar context and it is vulnerable to attacks due to its light-weight instrumentality [1]. Instead of working as a routing protocol, RPL serves in providing a framework that, as per the requirements, is compliant to the domain of the IoV applications [2]. Several risks are associated with IoV in the current communication paradigm which encompasses illegal access, breaching of data privacy, risk of virus and service attacks, and compromized confidentiality and reliability. Furthermore, factory usage explores the diverse range of attacks that are faced outside the tools and vulnerabilities of the system [3]. To avoid such attacks, a mechanism is required that can detect the attacks and prevent them from inflicting harm. [4]. In order to counter the attacks, evaluation of a variety of network attacks in IoV has been conducted and a number of IDs have also been made available. In IoV, DDOS has not been examined and the present IDS are not adequately designed to prevent the DDOS attacks.

To circumvent such issues, this manuscript provides a comprehensive analysis for the handling of DDOS attacks in various settings. Different types of IDS in IoV are discussed in this paper along with the IDS available for the DOS attacks. The study further provides the discussion on the importance of Artificial Intelligence techniques in constructing a defense system that is refined and effective in countering the DDOS attacks in the networks of IoV. Moreover, Artificial Intelligence provides low-cost solution and is

[*] Corresponding author.
E-mail address: sherazi@poliba.it (H.H.R. Sherazi).

https://doi.org/10.1016/j.suscom.2019.05.002
2210-5379/© 2019 Elsevier Inc. All rights reserved.

effective for making an immediate decision by evaluating system's configuration. The focus of such kind of study is to counter the resources and network bandwidth consuming agents who attack the target host by Artificial Intelligence-based techniques. The techniques considered in this study are, Immune System, Fuzzy Logic, Game Theory, Bio-Inspired and Semantic-Based AI and Q-learning.

Certain properties of the environmental setting are sensed by the physical things and then forwarded for further processing to the communication network [4]. The controlled devices in the IoV network are called 6LoWPAN or IP-Connected WSN. An IoV comprises of objects that are identifiable and has the ability to sense the setting that are presented in as well as the host devices. They transmit the sensed data to the Internet. The security of IoV becomes much more challenging due to the fact that the resources are highly controlled, and the devices are globally connected [5]. The security services that are deemed necessary for IoV are Confidentiality, Integrity, Availability, and Authenticity. An attempt to take over the resources and bandwidth of legal users by an attacker is known as a DDOS attack. These attacks commonly involve creating huge traffic that allows the attacker to consume the resources of the network, bandwidth and the CPU time of the targeted host. For instance, SYN flood, DNS flood, Ping flood, UDP flood, ICMP broadcast are common types of DDoS attacks [4].

The rest of the manuscript is organized as follow: Section 2 discusses the state of the art of various security approaches. The proposed system model is described in detail in section 3. Section 4 presents the simulation results and discussion. Finally, section 5 concludes the manuscript.

2. State of the art

2.1. Security settings for IoV based networks

In IoV, the number of connected vehicles keeps increasing that brings new requirements (such as seamless, secure, robust, and scalable information exchange among vehicles, human, and roadside infrastructure) with time. The IoV is built on the basic communication network and it is exposed to the risks which already exist in the communication system. These risks include attempts of illegal accessibility, data prying, virus attacks and other breaches of system and data privacy. The IoV subsists in a setting which consists of network construction, network interconnection, internetwork verification and handling other security issues. Such a setting enables it to be subjected to DoS attacks, and other system outbreaks such as a man in the middle attack, asynchronous attack, conspiracy attack and other similar occurrences. The IoV are complex systems having a wide number of devices, numerous data collection formats, and heterogeneous characteristics bearing data information. This complexity promotes issues of network security and contributes to network congestion when large number of nodes are involved in data transmission, which results in service denial attacks [3]. Unfortunately, as vehicles become increasingly automated and connected with the outside world, they tend to face growing security threats [3]. The most significant security services that are deemed necessary for IoV are briefly described below:

- Confidentiality: An attacker can easily intercept the message travelling from the source to the receiver and can easily fabricate the content. It is imperative that the data is hidden from all nodes of relaying in order to have a secured communication in IoV. To ensure this confidentiality, encryption/decryption can be utilized [4].
- Integrity: It is critical that the message does not get altered while traveling from source to destination. It should be received in its original form as sent by the sender. There should be no change in the message while passing [4].
- Availability: The continuous availability of the services provided by the data is important for the regulation of IoV and easy accessibility of data at the time of requirement. This requires detection and then prevention of intrusion to ensure the availability of the service [4].
- Authenticity: For transparent and authentic interaction, the users should be able to identify the identity of each other to ascertain that they communicating body is the same entity who they claim [4].

The significance of the stateless and stateful signatures is exploited by an ant-based framework. This provides preservation to the legitimate packets and discards the packets that are contaminated. In this process, the Ant-Based Routing Algorithm is utilized. The DDoS Ants detect the attack when either change occurs in reliability or the threshold value gets exceeded by buffer size. The unusual rise in traffic of the network is detected by the DDA. Cooperative Fuzzy Artificial Immune System (Co-FAIS) is discussed by Shamshir Band *et al.* [6] stating that the system keeps looking into the data from the network, inspecting the behavior of the sensor. The system comprises of six modules Sniffer Module, Fuzzy Misuse Detector Module, Danger Detector Module, Fuzzy Q-learning Vaccination Module, Cooperative Decision-Making Module and Response Module. This study provides a protection system for the DoS attack on WSN. The paper considers some important issues such as; fast growth of wireless sensors and providing security to sensor nodes.

2.2. Artificial intelligence and machine learning based methods for detection of attacks

A consecutive issue highlighted in the detection of the attack is the selection of the features that are most effective for the classification. The process of feature selection is a fundamental step in the Data Mining method's pre-processing. In the network intrusion system, various features are utilized that are generated by the consumption of packet headers, payload or handshaking of the protocol. Furthermore, the selection of feature causes decline in the data dimensionality and improvises the performance classification in terms of speed. The issues of large memory and disk usage can be faced when all features are consumed, making the process of the detection rather slow. The purpose of feature selection is to choose the features that are most representative and bear most discriminative power in the context of the dataset. The features used in this research study are extracted through the software Network Measurement and Accounting System. This software is used in cumulating related packets and form 43 features that are flow-based (i.e., feature extraction). This tool is amenable as well extensible for the measurement of the network. It produces flows and implements modules of packet processing in every single flow. Flow is deemed as a sequence of packets passing through an observation point from a particular source to a destination in the network during a precise time period. A hybrid method is implemented for the selection of feature in this research study. The search method that is found suitable for the optimization is the Genetic Algorithm (GA) that maintains an array of solutions.

This method regulates the search until it finds the best possible solution, or a situation erupts that terminates the process. The GA was first used by John Holland for developing a system in the computer world. The solution collection presented in the GA is showcased by chromosomes that comprise genes. Properties of one solution are represented in each chromosome and the best chromosome fit for the function is selected by the algorithm. The amount of similarity of the chromosome is presented in the fitness function to answer of the search problem. New chromosomes are created by algorithm through crossover mechanism of chromosomes in order to answer the search problem. There are two types of crossover; the One-point and the Two-point crossover. An alternate mechanism is used by an algorithm as mutation to prevent local results. Only those chromosomes survive that serve the purpose. For the feature selection of DDoS attack detection system, GA along with the Artificial Neural Network classifier is used. The proposed model is a kind of wrapper feature selection method. A fitness function is applied to score feature subsets by GA to determine the best chromosome in the chromosome selection phase. In the representation of feature subset, the i^{th} feature is allowed for participating in the classification if it equals to 1. Similarly, if it equals to 0, it is not deemed appropriate in classification. The crossover rate in this research is 0.6 and the population size is 20. The mutation and other parameters are based on the de-fault values of application.

In the proposed wrapper method, the accuracy of classification serves as fitness function; stating that selected features in each generation are implemented to calculate the accuracy of classification. For each new subset, the system is trained and tested on dataset. Out of the ten-fold cross validation, one-fold is used for the dataset testing, and the remaining nine folds are utilized in training the dataset. If the condition of termination is not met, a new generation is formed using crossover and mutation operation. The trend continues until best feature is found in terms of accuracy. IP address, port number, and protocol-related features are eradicated for the improvisation of the robustness of the system. An AML technique known as Artificial Neural Network (ANN) is implemented to detect the DDoS attack. This has the benefit of having fewer parameters to optimize for training networks. Inspired by the human brain, it comprises of several neurons. ANN applies the concept of exchanging pulses between neurons and their link with the synaptic weights' input to generate output as it occurs in the brain. This solves the classification problems.

Input, hidden, and output layers are present in ANN model. These layers are exemplified by the "Multi-Layer Perceptron (MLP)" which is a class of ANN technique that maps the set of input to the set of suitable output. Irrelevant characteristics are removed from the flow and only best features are used in the input layer of ANN system. They are extended to the hidden layer and eventually presented in the final output layer. In this research, the default parameters mentioned above, are used for "Multi-layer perceptron".

Traditional methods are not efficient for detection of the DDOS attack. A new hybrid method for detection, GA and ANN, was proposed. The best features were extracted and implemented using GA feature selection method. To improve the detection and accuracy rate of the system, "Multi-layer perceptron" of ANN was used. The results of this research are more accurate than previous researches conducted, and similar lines can be implemented in future for more experiments on various datasets to examine the proposed method's robustness.

In order to counter the attacks, evaluation of a variety of network attacks in IoV has been conducted and a number of IDs have also been made available. In IoV, DDOS has not been examined and the present IDS are not adequately designed to prevent the DDOS attacks. To highlight such issues, this paper provides a comprehensive analysis of the handling of DDOS attacks in various settings. The study further provides the discussion on the importance of Artificial Intelligence techniques in constructing a defense system that is refined and effective in countering the DDOS attacks in the networks of IoV. Moreover, Artificial Intelligence provides low-cost solution and is effective for making an immediate decision by evaluating the setting. The focus of this study is to counter, using Artificial Intelligence-based techniques, the resources and network bandwidth consuming agents who attack the target host. The techniques considered in this study are; Immune System; Fuzzy Logic; Game Theory; Bio-Inspired technique; Semantic-based technique and Q-learning.

The network security approaches, intrusion detection system in particular, collect the data required for monitoring the parameters of the network and serve in identifying the attacks and the attackers. Controlled resource devices are inclusive in IoV which makes IDS' hybrid architecture more suitable for it. The centralized module can function on 6BR. For a smaller module, computational aspects can be installed on the sensor nodes which contribute to the collection of network data. The IDS system, for the detection of the attacks uses methods such as Event Detection Based IDS [1,7], Signature Detection Based IDS [7], Specification Based IDS [1], and Host Based IDS [1]. Ant-based framework is discussed by Juneja *et al.* [8] that lacks the importance of signatures such as stateless and stateful by preserving the valid packets only and eliminating the contaminated packets.

Selective forwarding attack takes place when selective packets are forwarded [5,7]. The sinkhole attacking node in Sinkhole attacks, advertises a routing path, posed as beneficial to the target host, and attracts the nodes to track the traffic through it. Parent fail-over and rank authentication technique has been evaluated by the IDS system to defend against this attack [1]. In Hello Flooding attacks, the attacker initiates a HELLO message broadcasted to various nodes. The node selected should be within the transmission range. However, this sort of attack can-not last for long in an RPL network and is then removed by Global and Local repair mechanism of RPL [9]. The wormhole attack can break the barriers of RPL. Its purpose is to disturb the topology of the network and affect the traffic flow [10]. In the clone IDS attack to access gain to the traffic that is destined towards the node of the victim, attackers form clone IDs. This type of attack is possible for RPL network. To minimize the effect of this attack, tracking number could be used for each identity and can identify the cloned identities [1]. In the black hole attack, attacker node drops the packets discreetly and causes all the nodes in the network routing to be dropped [11]. Denial of Service Attack is an attempt to disable the resources to the target the end-user. In RPL, using the IPv6 UDP, such an attack can bring packet flooding [12].

An early detection technique for the DDoS attack was presented by a different researcher. A comprehensive study has been conducted by Saraswati *et al.* [13] about the DoS attacks in the Wireless Sensor Networks (WSN). It classifies them as per the underlying techniques. In WSN, protected transaction is complex. The mentioned research has developed detection techniques which are efficient in denial of service attacks. To detect DDoS attacks in the wireless sensor environment, Jindal *et al.* [14] suggested an effective method. In this research, the provided method is deemed far more efficient than the existing method. The suggested method uses NS-2 simulator and the performance enhancement is observed in the context of energy consumption, delay, quantity, packet loss, and packet delivery ratio. The DoS attacks reduce the WSN's capabilities which lessen their functioning time span. A protective system to counter the DoS attacks on WSN is proposed by Patil *et al.* [15] which enhances and refines the accuracy rate of the attack. Furthermore, the system provides for reducing the rate of false alarm and detects diverse range of DDoS attacks. The attack technique is mostly based on soft computing, game theory, artificial intelligence and approaches of multiple agents. Moreover, fuzzy Q-learning algorithm is used in the soft computing-based approach.

3. Proposed model

In the proposed model, the IoV network comprises of a clusters (C), cluster heads (CH), and member sensor nodes (n) in the hierarchical order as shown in the Fig. 1. Sink node in each cluster is

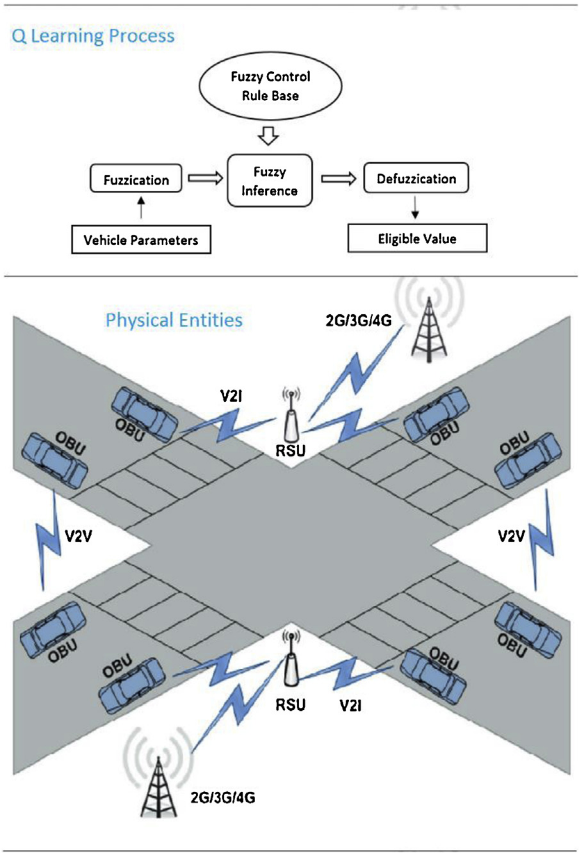

Fig. 1. A typical IoV Network Topology.

Table 1
Performance Parameters.

Parameters	Variables	Ranges
Communication Channel Efficiency (bps)	Low, Medium, High	0 - 100
Buffer Size (Kb)	Low, Medium, High	4 - 7068
Time Response (ms)	Low, Medium, High	0 – 120
Count (ms)	Low, Medium, High	1-3%
Pattern (P)	Bad, Average, Good, Excellent	N/A

considered as the cluster head and monitors the behavior of sensor nodes in the network through gathering the data from various sensor nodes and delivering information related to sensor nodes attack to the heads. Cluster head, in response, sends the coordinate data of sensor nodes to 6BR that serves as the border router in the framework. Sensor nodes are monitored into cluster grouping, whereas each cluster is represented into distributed system formation. For switching of sensor nodes (n), 6BR router is placed in the IoV network. The data is collected from the n^{th} cluster head (CH_n) by 6BR and serves the objective of performing Intrusion Prevention System (IPS) of ongoing traffic at 6BR level for the prevention of DDOS attacks through consuming fuzzy and Q-learning algorithm presented in Table 3. The DDOS attack uses system resources as well as resources of the end users. These resources comprise of the nodes that are present in the system. A subset of sensor nodes is examined in the previous DDOS attack cases, equivalence prevented IPS to perform effectively in stopping attacks on live traffic. In the IoT, 6BR bears sufficient capacity and resources for the IPS algorithm enduring.

In Fig. 2, five modules of Intrusion Prevention System (IPS) are displayed that perform an inspection of live traffic and analyse packet features using fuzzy logic. Furthermore, this system employs Q-Learning algorithm for the decision making in improving the traffic detection efficiency. This work comprises of two innovative features; inspecting real-time traffic for IoV network and examining DDOS attack through artificial intelligence and contraption learning algorithm. To the best of author's knowledge, such techniques have never been studied and adapted for IoT based networks in the past.

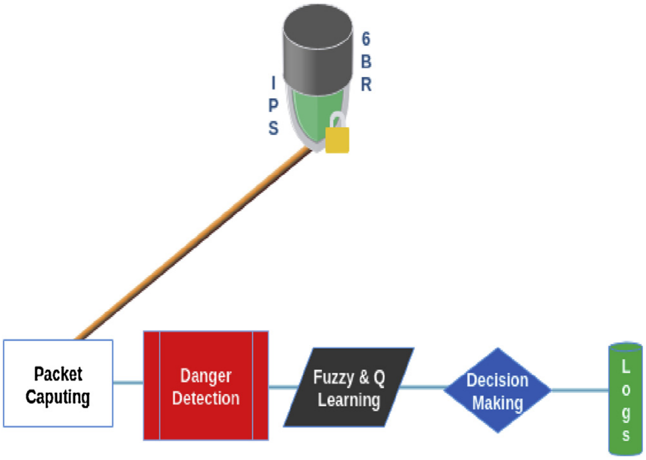

Fig. 2. Online Packet Inspection Module.

3.1. Packet capturing module

The packets from the network movement are held by the Packet Capturing Module and each packet's constituents are inspected. The data is pried online and is transferred for attack investigation in the detection module. The pried data is then put into the inspection system and results are saved as a log file. These packets are analyzed in IPS based network using the fuzzy rule that pre-processes the features of the packet.

3.2. Detection

A baseline is defined to detect malevolent packet on the network which attempts to pass through IPS. This baseline has a threat profile which helps with the decision making in the context of the value of threshold of suspicious network packet attacks in existing situations. Four tuple functions are used to define the signal attribute in the line network detection. These functions are; Communication Channel Efficiency (C2e), Response Time (T_r), Buffer Size (B_s), and Count (C_o). The C2e highlights the communication channel consumption efficiency evaluated in bits per seconds. Furthermore, T_r refers to the time difference between two connections operating simultaneously. Buffer size (B_s) states the distance between the source and the final point. Finally, C_o determines the number of connections from the same host in last two seconds. Detection module's primary concern is to compare the packet profile in contradiction to the function value of decision that is preserved in a database and explores for conceivable aberrations.

The reliability index of Packet Information (PI) is calculated by extracting the mean of all the mentioned values.

$$TP = \text{Packet}\quad \text{Informatin} = \left(C2^e + Tr + Bs + \frac{Co}{4} \right) \tag{1}$$

Table 1 describes the threat Profile Etymology and acronym of variables for each parameter.

To analyze the vulnerability of a malicious packet, the ranges used are given in Table 2.

If (TP >= Threshold Value) then the packet will be examined by fuzzy logic based expert system. The packet reliability probability is

Table 2
Trust Classification.

	Variables	Ranges
TP =	0 - 10	High Trust
	10 - 20	Medium Trust
	20 - 50	Low Trust
	> = 50	Threshold Value
	0 - 10	High Trust

Table 3
Proposed Algorithm for Q-Learning.

Algorithm 1: Total packet probability through Q-Learning Algorithm Design

```
$P_{total}$ (i); where (i) is the id of a packet.
if ($P_{total}$ (i) > 0 &&< 0.5)
    Assign Fuzzy Min to $P_{total}$ (i)
Else;
    Assign Fuzzy Max to $P_{total}$ (i)
Suppose a (i) is the action to be taken on $P_{total}$ (i).
While ($P_{total}$ (i) (does not belong to) Fuzzy Min)
Begin Calculation:
Q ($P_{total}$) (i) //Assign to quarantine (j)
Check if other packets exist in queue memory.
Calculate percentage difference between (i) and other packets.
If (difference > 20)
    Drop Packet
Else if (difference < 20)
    Quarantine
Else;
    Forward.
```

achieved by regular broadcast ratio. To obtain reliability, following calculation can be made:

$$P_{rel}= \frac{P.I}{\left(\frac{No.\,of\,Packets}{sec}\right) * Bandwidth} \tag{2}$$

If the packet information probability lies within the range of 0.5 and 1, the information is deemed reliable and the packet is forwarded without any further action in the IoV Network. In other case, if the probability is between 0 and 0.5, packet will be considered ambiguous for being malevolent.

3.3. Fuzzy and Q-Learning methods

The problems related to DDOS attacks are addressed several times in the literature. In situations where values are constructed on estimation and complete information is available, fuzzy logic controller aids in the decision making. Detection frameworks based on fuzzy logic have the capability to calculate the ambiguous information availability. These frameworks are appropriate for the decisions' description, but face difficulty in obtaining rules that would allow the decisions to be made. To improvise the behavior exploration drawbacks, fuzzy logic along with the neural framework in the context of adaptive neuro-fuzzy is suitable to identify the abnormal behavior by tuning the rules. Significant advantages that neuro classifier bears are that of strength and flexibility. However, extensive computing resources are consumed during fuzzy alarm connection performance in a wider scale of the wireless framework.

Reinforcement learning is considered as a substantial method. This is because of its ability to adopt new techniques of attacks online and unguided learning. Moreover, it has the tendency to alter the policies without having to deal with complex approaches to mathematics. It is verified to be proficient; particularly in the situation of live traffic fault detection and in cases where no assumption is made for the previous system's behavior. A drawback of reinforcement learning is the inability of storing data of the agent. This has motivated the researcher to develop intelligent systems that would be able to utilize fuzzy logic systems to tackle the issues related to memory and detection accuracy [16].

3.4. Fuzzy alleviator module (FAM)

The primary obligation of the FAM model is to keep the information updated regarding thresholds, profile databases and etc. In the closely observed environment, suggested model detects the capacity of a system to respond and counter the attacks. For quick detection of attack in a live traffic, concept of Fuzzy Q-Learning is utilized in this study as proposed by Shamshirb [16]. In the proposed scheme, fuzzy min-max method was applied. In the fuzzy min-max action selection and reward operate with Q-Learning to detect the behavior of the attack. Learning capabilities are reinforced using Fuzzy and Q-Learning (FQL) that showcases the optimization based on FQL as illustrated in the block diagram in Fig. 3. The proposed strategy for the detection of active mode attacks is based on FQL logic that includes and monitors the attack prior to conceding the IoV cloud's sensor node. The design of the proposed optimized system alters the withheld traffic into subsequent inputs comprising of four sets of variables. These sets are investigated by the detection framework. In case the threshold value matches the value of threat profile, maliciousness is detected in the packet.

The probability of the packet is checked by Fuzzy logic and min-max is assigned based on the ratio of packet's total probability, P_{total}, in regard to the id (represented by i) of the packet. The total probability of the packet determines the course of action required to conduct the calculation of Q-Learning that decides the eminence of the packet. This status is classified as Quarantine, Drop, and Forward.

3.5. Response module

As for the selection of best strategy, 6BR device is utilized for the exploration of approaching attack and countering it. Irrespective of the commencement of the attacks on more often basis or not, the IPS has the tendency to modify its learning parameters for the detection of the upcoming attacks. The mechanism of detection proposed, in this study, identifies signals of danger at 6BR level and conducts the virtual investigation of every single packet that passes the network in order to avoid the DDOS attack. If an abnormality is detected in the packet, it gets dropped by the Decision Module and its logs get stored in order to prevent similar attacks in future. If the attacking body is successful in reaching the IoV network's sensor node, it gets directed to the sink node and then towards the 6BR router for the recording of the pattern. Identification is conducted in two positions; internet to 6BR's edge path and commencing of detection on both node as well as in the Private Cloud of IoV. The real time traffic and the behavior of the sensor are inspected in the first phase of detection. Attack's dataset comprises of complete packet and system usage profile that includes; usage of CPU, memory load, bandwidth, size of packet, packets frequency generating from the same host. When abnormal packets are delivered to 6BR, sink nodes are inspected and compared in terms of parameter to deduce the normality level of packets. If the match is found in the pattern that's saved in 6BR database, coordinating nodes are inactivated in the situation of attack.

4. Performance evaluation

To investigate the performance and identification of a correlation between routing protocol and FQL, the situations of DDoS attacks are the ones that are considered in an active mode. The presence of attacker characterizes the flooding attack or the DDoS attack. Flooding, within an attack, utilizes the network resources

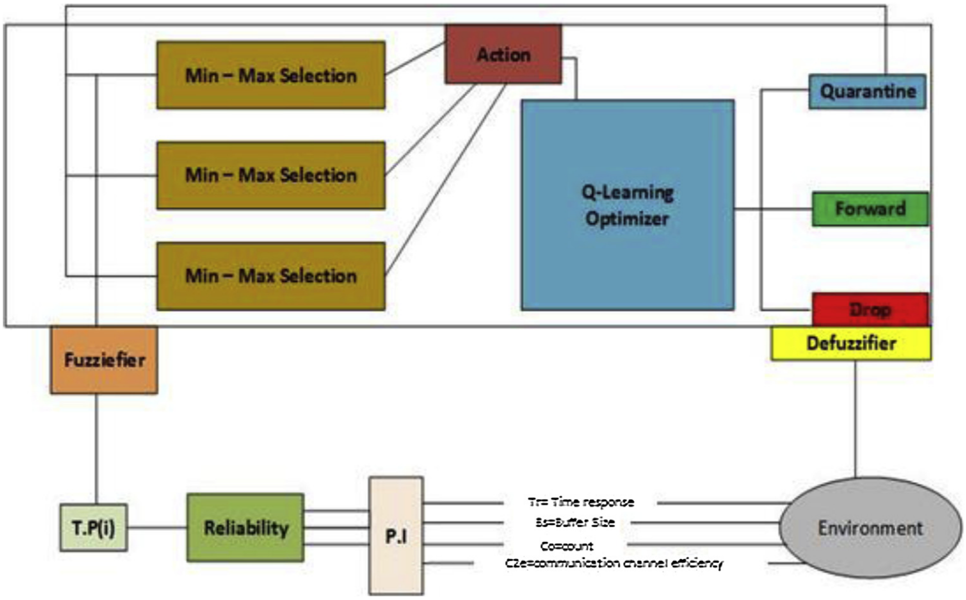

Fig. 3. FQL Optimized Block Diagram.

and formulates interruption inside the network and disables the sources. In the simulation, a protocol is used in the active mode to observe the process more precisely. It is also implementable to coordinate with other associated concerns related to network consumption. Further, it is important to discuss that parameters and values, at this time, are yet to be decided.

4.1. Attack strategy

This section is focused to formulate simulated data for attack and scrutinize the attacks' behavior in a quantitative context in the UDP layer of protocol. In normal UDP in the existing experiment, traffic is considered primarily, following which the intensity of attack in relation to UDP traffic. The consumption of energy prior and after the attack was investigated and in order to ignite a flooding attack, an algorithm was designed for the attack. After formulating a virtual attack, dataset of the attack was gathered in the module of IPS and finally, the algorithm was implemented on the acquired dataset.

4.2. Measurement

To compare the attacked data, it is important to analyze it when it is passing through a normal course. For such purpose, virtual inspection using FQL algorithm is considered. There is need to convey data of the attack regardless of the consumption of proposed remedy for the issue. In this precise practical attempt, the consumption of total channel before and after the assault is experienced along with the number of packets approaching from a constant source in two-minute time frame along with the packet's port number.

4.3. Results

Fig. 4 shows the comparison of proposed solution and the solution using existing techniques. A comparison of proposed and existing solutions in term of average buffer usage is also performed (see Fig. 4). The simulations have been performed by using well-known NS-3 simulating environment.

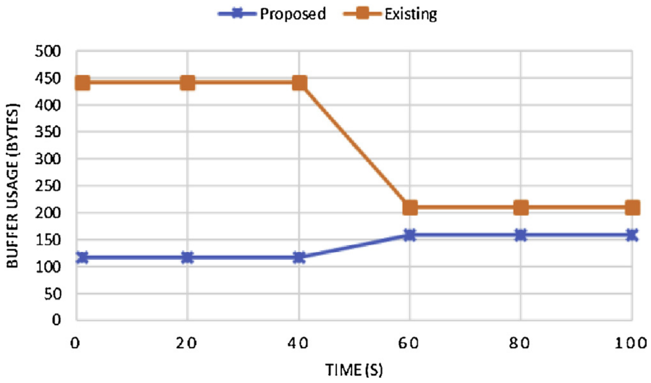

Fig. 4. Buffer Size Usage on 100 Sensor Nodes.

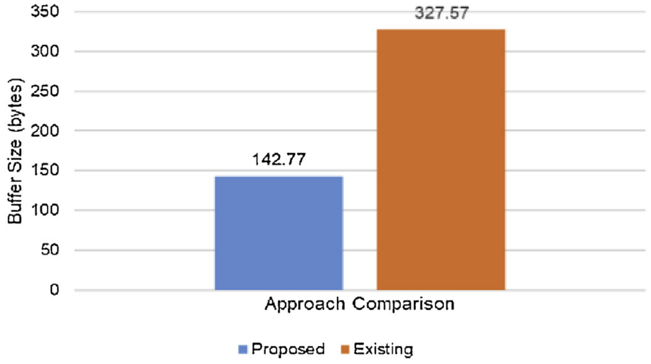

Fig. 5. Average buffer usage on 100 sensor nodes.

Fig. 4 shows the comparison of the buffer size usage between existing model and proposed model. Buffer size is an important factor in calculating the computation overhead for sensors. Lesser buffer size ensures efficiency of the algorithm. After few hikes the buffer size in existing technique is increasing exponentially, as shown in Fig. 5. While the proposed technique due to late FQL implementation has comprehensively decreased the buffer usage and hence increasing the battery life of the sensors.

The energy consumption in existing technique is on a higher end that goes on to 11.8 J while in proposed model, it has inclined up to a maximum of 4 J and remains constant thereafter (see Figs. 6 and 7).

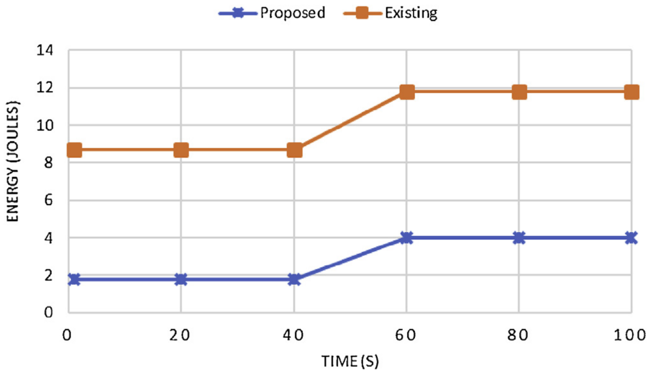

Fig. 6. Energy consumption in both proposed and existing techniques.

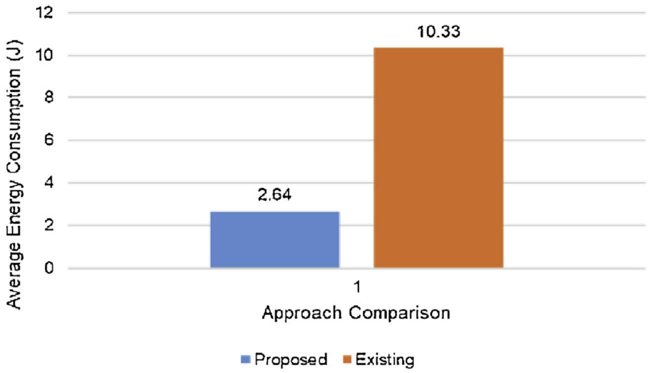

Fig. 7. Average Energy Consumption in both proposed and Existing Technique.

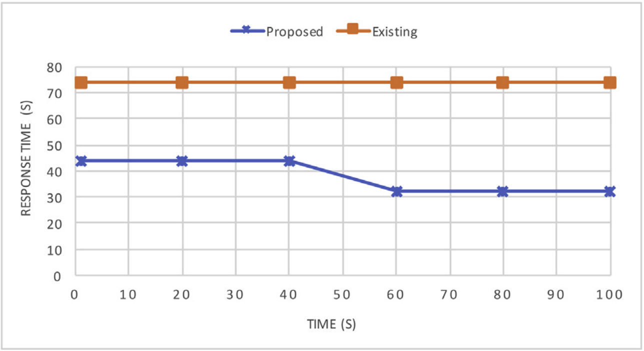

Fig. 8. Response Time of 6BR Router using Proposed and Existing Technique.

The response time of 6BR router in proposed model is decreasing during the training stage and eventually decrease showing the completely trained system (see Figs. 8 and 9).

In Fig. 10, the existing technique shows throughput in the end because of exhausting sensors while the proposed solution shows an increase in throughput till almost link speed of 1.6kbps.

5. Conclusion

Security and privacy issues in IoV applications have always been in spotlight. In this paper, we have discussed Intrusion Prevention System (IPS) based protection and proposed a solution based on Fuzzy Logic and Q-Learning. Moreover, the interaction between attackers and IPS has also been analyzed. The analysis has been performed on the basis of 4 tuple variables. This system comprises of Fuzzy Logic and Q-Learning algorithm and implemented on 6BR device which checks every internet packet actively (IPS based inspection). Previously, passive (IDS based inspection) approach has been used in RPL based IoV networks. It has been identified that DDoS attack can cause congestion in IoV communication because of flooding packets. The model such as Fuzzy Alleviator Model and Q-Learning strategy that are construed as multi-agent can provide defense against a single attacker. Such models are also useful in self-learning from the history of the attacks that aids in the decision making. Our proposed scheme, as a method in IPS, is a helpful tool for improving security in the next-generation complex heterogeneous networking against the sophisticated attacks for implementing a sustainable vehicular network. A future work is planned to extend the proposed method by incorporating data from various attack types. This paper gives a brief introduction to typical attacks on IoV, security issues and presents a mechanism against attacks on IoV and similar systems that are highly dynamic in nature.

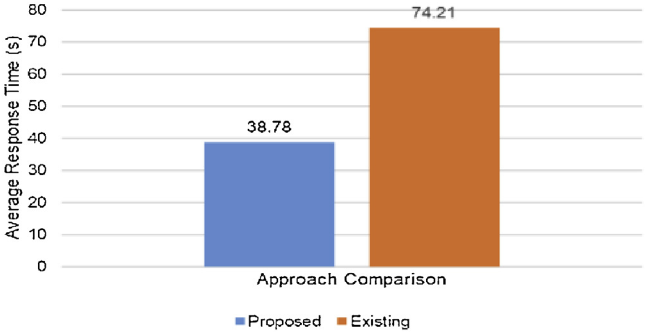

Fig. 9. Average response time of 6BR router using proposed and existing techniques.

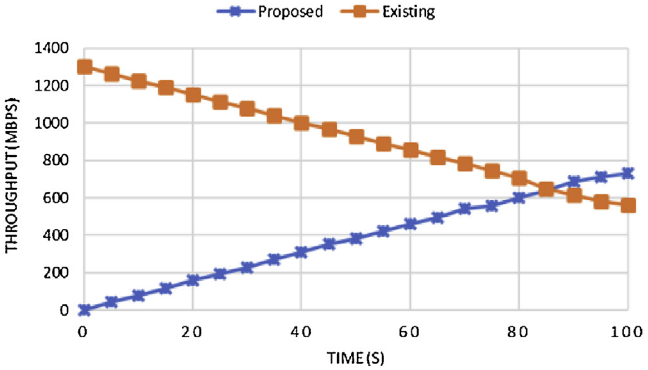

Fig. 10. Throughput evaluation using proposed and existing solutions.

References

[1] P. Pongle, G. Chavan, A survey: attacks on RPL and 6LoWPAN in IoT, January, 2015 International Conference on Pervasive Computing (ICPC) (2015) 1–6.

[2] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1294–1312.

[3] G.O.U. Quandeng, L.I.U. Yihe, Y.A.N. Lianshan, L.I. Yao, Construction and strategies in IoT security system, in: IEEE International Conference on Green Computing and Communications and IEEE IoT and IEEE Cyber Physical and Social Computing, 2013, pp. 1129–1131.

[4] K. Sonar, H. Upadhyay, A survey: DDOS attack on internet of things, Int. J. Eng. Res. Dev. 10 (11) (2014) 58–63.

[5] L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the rpl-based internet of things, Int. J. Distrib. Sens. Netw. 9 (8) (2013), 794326.

[6] S. Shamshirband, N.B. Anuar, M.L.M. Kiah, V.A. Rohani, D. Petković, S. Misra, A.N. Khan, Co-FAIS: cooperative fuzzy artificial immune system for detecting intru-sion in wireless sensor networks, J. Netw. Comput. Appl. 42 (2014) 102–117.

[7] A. Le, J. Loo, Y. Luo, A. Lasebae, Specification-based IDS for secur-ing RPL from topology attacks, October, in: Wireless Days (WD), 2011 IFIP, IEEE, 2011, pp. 1–3.

[8] D. Juneja, N. Arora, An ant based framework for preventing DDoS Attack in wireless sensor networks, arXiv preprint (2010), arXiv:1007.0413.

[9] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schönwälder, A study of RPL DODAG version attacks, June, IFIP International Conference on Autonomous Infrastructure, Management and Security (2014) 92–104.
[10] F.I. Khan, T. Shon, T. Lee, K. Kim, Wormhole attack prevention mecha-nism for RPL based LLN network, July, 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN) (2013) 149–154.
[11] K. Chugh, L. Aboubaker, J. Loo, Case study of a black hole attack on LoWPAN-RPL, August, Proc. of the Sixth International Conference on Emerging Security Infor-Mation, Systems and Technologies (SECURWARE) (2012) 157–162.
[12] P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based internet of things, October, 2013 IEEE 9th International Conference on Wireless and Mobile Compu-Ting, Networking and Communications (WiMob) (2013) 600–607.
[13] A.P. Abidoye, I.C. Obagbuwa, DDoS attacks in WSNs: detection and countermeasures, IET Wirel. Sens. Syst. 8 (2) (2018) 52–59.
[14] S. Jindal, R. Maini, An efficient technique for detection of flooding and jam-ming attacks in wireless sensor networks, Int. J. Comput. Appl. (2014) 0975–8887.
[15] S. Patil, S. Chaudhari, DoS attack prevention technique in wireless sensor net-works, Procedia Comput. Sci. 79 (2016) 715–721.
[16] S. Shamshirband, N.B. Anuar, M. Laiha, M. Kiah, S. Misra, Anomaly detection using fuzzy Q-learning algorithm, Acta Polytech. Hung. 11 (8) (2014) 5–28.