Contents lists available at ScienceDirect

Advances in Engineering Software

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

Detection and prevention of man-in-the-middle attack in iot network using regression modeling

N. Sivasankari [a,*], S. Kamalakkannan [b]

[a] Research Scholar, Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies, VISTAS, Pallavaram, Chennai, India
[b] Associate Professor, Department of Information Technology, Vels Institute of Science, Technology & Advanced Studies, VISTAS, Pallavaram, Chennai, India

ARTICLE INFO

Keywords:
Internet of things (IoT)
Regression modelling
Man-in-the-middle (mitm)
End-point man-in-the-middle attack

ABSTRACT

Security is the primary concern in any IoT application or network. Due to the rapid increase in the usage of IoT devices, data privacy becomes one of the most challenging issue to the researcher. In IoT applications, such as health care, smart homes or any wearables, transmission of human's personal data is more frequent. Man-in-the-Middle attack is one in which outsiders eavesdrops the communication between two trusted parties and steal the important information such as password, personal identification number, etc., and misuse it. So, this paper proposes a Regression Modelling technique to detect and mitigate the attack to provide attack-free path from source to destination in an IoT network. Three machine learning techniques Linear Regression (LR), Multi-variate Linear Regression (MLR) and Gaussian Process Regression (GPR) used and performance of these three algorithms analyzed on various metrics and shown Gaussian Process Regression provide higher rate for detecting the attacks and produces the lower rate for misclassification of attacks.

1. Introduction

Today we live in the digital era. Internet enters every human life in the world. Due to the popularization of internet, the next advancement 'Internet of Things' comes into existence. That is, one device will be able to communicate with other device without human intervention. Study shows that IoT market starts with 2 billion objects interconnected in the year 2006 and at 2020 it increased to 200 billion. The drastic growth is due to the intelligence of IoT devices, so it is adapted in almost every field like education, health care, agriculture, finance, smart home, smart cities, smart vehicle, etc., IoT environment consist of heterogeneity of devices, networks, protocols, and standards. No network is free from security threats and vulnerability. The security loopholes of IoT system create various security threats to the different IoT layers. Since IoT is involved in many areas such as medical, power plant, and home automation, attacks on such crucial applications may cause severe consequences. OWASP published several in-build vulnerabilities, i.e., weak passwords, insecure network and cloud services, usage of outdated components, insecure default setting, data transfer and storage of IoT devices can allow the attackers easily to penetrate the system.

Regarding IoT, attacks generalized into four categories: Physical Attacks - targets the hardware of an IoT system, Network Attacks - used to extract large amount of data remotely, Encryption - finding the encryption key and steal the data and Software attack - accessing the entire software system by installing malware, virus, phishing, injecting malicious code. The following are the various common cyber threat attacks in IoT:

Botnets: Botnets are collection of compromised computers remotely controlled by cybercriminals to carry out various swindles and cyber-attacks such as stealing private information, exploitation of data, phishing emails, and DDoS attacks. The rapid growth of IoT, led to more devices connected to the Internet and increase the attack vector possibilities. Botnets as well as Things Bot have two common characteristics: internet enabled and transfer data automatically via a network. They are difficult to detect because the user has no knowledge that the device is compromised. Botnets follows command-and-control model in which central server controls the bots in the network.

Man-in-the-Middle: Man- in- the- Middle (MitM) attacks occurs when the hacker breaches communication between two end system by injecting a malicious node between the legitimate nodes or by targeting the communication protocols in IoT network. Through the MitM concept, the hackers can alter the traffic flow, reconfigure the network topology, create fake identities, and generate malicious and false information to compromise an IoT system. The variants of MitM attack are

[*] Corresponding author.
E-mail addresses: sivasankari1985.n@gmail.com (N. Sivasankari), kannan.scs@velsuniv.ac.in (S. Kamalakkannan).

https://doi.org/10.1016/j.advengsoft.2022.103126
Received 26 February 2022; Accepted 20 April 2022
Available online 6 May 2022
0965-9978/

Table 1
Dos Attack at different layers.

Layer	Type of DoS Attack
Physical	Jamming Attack
Data Link	Collision
Transport	Flooding
Application	Path based

eavesdropping, Sybil attack, Wormhole attacks, Identity replication attack, Node replication attacks, etc.,

Eavesdropping attack is possible due to unsecured communication link to access personal data between two end devices. It is also known as sniffing or snooping attack.

If a weakened connection between an IoT device and server found, an attacker might be able to intercept network traffic and steal the possibly sensitive information that IoT devices transmit over enterprise networks.

Wormhole attack is an internal attack which is hard to identify. Attackers listens the activities of network without altering it.

Sinkhole attack creates network traffic by sending route request to neighbor node. It transmits fake information and collapses the entire network communication. It is the most destructive routing attacks in IoT environment.

Social Engineering: Social Engineering is the act of manipulating user and getting their confidential and sensitive information and gain illegal access to data. Attackers executes social engineering easily in IoT devices because IoT devices usually collect large volume of information, especially personal identification in case of wearables, health care to provide personalized and friendly services.

Denial of Services: DoS attack are common attacks in IoT systems. This happens when a requested service or resources is unavailable to the users. In a Distributed Denial of Service (DDoS) attack, many malicious systems are involved to attack one target. DoS attack can be possible in each layer of communication and it is shown in Table 1.

Privilege escalation: Attackers gain access to IoT resources which are protected from user or an application by exploiting flaws in design, device bugs or operating system bugs or through configuration of application-software.

Brute Force Password Attack: In Brute-force attacks, access to the device is possible due to the weakness of IoT device passwords.

Firmware hijacking: Firmware hijacking makes the attackers to hijack the device and download the malicious software. It is made possible, when an IoT devices download the firmware updates from an illegitimate source.

Physical tampering: In an IoT devices deployed environment, where the enterprise fails to control the device and the people who can access it, there exists physical threats. Moreover, globally, attacks emerge due to continues rapid expansion of IoT. Attackers make use of compromised IoT nodes to gain access to network and move more deeper into it by passing variety of security controls. Finally, attackers can send sensitive information to themselves via IoT devices.

Ransomware: Ransomware is one of the well-known bad attacks in IoT. Hackers can encrypt the critical data of the user and demand a ransom for decrypting the same. For example, the intruders can tamper a smart health care system and send a notification to the owner to pay a ransom. It can also use to attack IIoT.

In IoT network, various attacks are possible and it leads to security and privacy issues. Implementing legacy network attack detection techniques is not possible due to the resource constraints of IoT devices and of different protocols used. The proposed work focuses on detecting End-point Man-in-the-Middle (MitM) attack using regression analysis:

- Simulating an IoT nodes and generating both normal and adversary (MitM) data traffic using NS2 tool.

Table 2
Literature Review.

S. No	Reference and year	Problem	Solution	Remarks
1	G. Hatzivasilis. et.al., 2021	Botnet attacks in IoT - leads to cyber attacks	An end user awareness system that informs botnet infection at machine side	Identifying the infected node and send notification
2	Ryan Heartfield.et. al., 2021	Security to smart home: new devices, different users	IDS for smart home-autonomous - take decision on its own based on changing condition	Decision making - classification problem
3	Weizhi Meng.et.al, 2020	Internet of Medical Things (IoMT) - insider attacks- trust management?	Investigate performance of blockchain for IoMT. Blockchain applied to Bayesian inference-based Trust management	Incorporates blockchain technology
4	A. Mourad. et.al, 2020	Heavy computation for IDS -unsuitable for AI powered self-driving vehicles-centralized cloud computing-high latency-delay	Fog enable scheme - federated vehicle nodes	Fog computing focused on computation time
5	Hamed Haddad Pajouh, 2019	Due to diversity of IoT devices U2R and R2L - most challenging	Novel model - anomaly based - for detecting User to Root(U2R) and Remote to Local (R2L)	Anomaly based IDS
6	Laisen Nie.et. al,	Machine learning algorithms for hindering cyber-attacks on CPSs. Absence of labeled data from novel attacks makes their detection quite challenging.	Generative Adversarial Networks (GAN)-to detect cyber-attacks on cyber-Physical system (CPS)	IDS for CPS
7	S. Prabavathy. et.al., 2018	To detect the cyber-attack faster	Novel IDS - based fog computing using Online Sequential Extreme Learning Machine (OSELM)	Fog computing attack or non-attack
8	Parminder Singh.et.al.,	Current IDS for EoT are not intelligent to control false alarm	Intelligent IDS in Edge-of-Thing Ecosystem - deep learning classifier used	Dew computing used as a Service
9	Bighnaraj Naik.et.al.,	More possibility for attacks at edge. Need of IDS	Providing intelligent IDS in EoT teaching-learning meta-heuristic optimization used to obtain parameters for functional link neural net	Provide IDS for detecting attacks
10	Faezeh Farivar.et. at.,	Cyber-attacks in CPS Automatic deliberate of faults and maintain system	Hybrid intelligent classic control approach - focus inputs of non-linear CPS and IIoT	Provide solution for cyber-attack in CPS

(*continued on next page*)

Table 2 (*continued*)

S. No	Reference and year	Problem	Solution	Remarks
		performance at some acceptable level.		
11	Paulo Freitas de Araujo-Filho.et.al.,	Novel attacks detection is quite challenging. GAN-unsupervised approach. Attacks on CPS stopped before system compromised	FID-GAN: Fog-based, unsupervised IDS	Focused on attacks in CPS

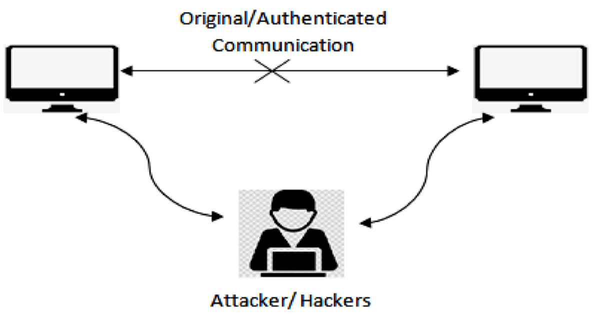

Fig 1. Man-in-the-Middle Attack.

- Three machine techniques such as Linear Regression (LR), Multi-linear Regression (MLR) and Gaussian Process Regression (GPR) applied to collected data set.
- Performance of techniques analyzed with both positive and negative measures.
- Proved that Gaussian Process Regression technique provides greater accuracy in detecting the attack while identifying the path between the source and the destination.
- The main contribution of the proposed work is as follows:
- To enhance privacy in IoT network by detecting Man-in-the-Middle attack.
- No need of central controller to detect the attack. Hence, each source node in IoT LAN finds attack free path (without MitM node) to the destination node on its own.
- Provides a higher detection rate of attack and lower false measures.

The remaining of the paper organized as follows: Section 2 includes Literature survey regarding various approaches for enhancing security in IoT networks. Section 3 depicts proposed attack detection framework. Section 4 discusses the experimental results of the proposed work and Section 5 concludes the paper.

2. Literature survey

The previous studies related to enhancing security in IoT environment is depicted in the Table 2 [1–11]

From the survey, it is clear that IoT environment still vulnerable to many attacks and researches are going on in many aspects. This research work is focused on detecting Man-in-the-Middle attack specific to end nodes attacker in IoT environment.

3. Proposed work

As the name implies, in Man-in-the-Middle attack, attackers play a role between two legitimate users as shown in Fig 1. In this, attackers eavesdrop the communication link and listen the conversation between two targets. Man in the Middle attack is possible in two ways: 1) by placing an adversary node between the legitimate nodes or 2) by injecting malicious code or software on the target host machine.

For instance, think where a malicious user takes the control of heat monitoring device and fake the data to overheat the machinery and stop the production in manufacturing industry where Internet of Things incorporated.

Growth of IoT devices is increasing drastically in the past few years. IoT not only adopted in manufacturing, it widely covers major areas such as hospital, agriculture, education, transportation, home monitoring and controlling etc., where huge amount of personal information is generated and transferred. Man in the Middle is about sending fake information, stealing the data, altering the messages/data, or impersonating the user or the devices we think of talking about. Due to the constraints in the features of IoT devices, the standard security measures for prohibiting MitM attack is not suitable for IoT environment and thus it is more vulnerable to attacks.

MitM attack will be made possible in three ways as depicted in Fig. 2:

End-point MitM: Attacker node will be one of the end host nodes.

In-line MitM: Attacker node placed between the central controller/router and the external cloud storage or server. The messages redirected via attacker node.

In-point MitM: Attacker will replace the central controller or the router

The proposed work emphasis on detecting End-point MitM attack where end host node will become an attacker node. In this work, different kinds of regression analysis performed based on the path of the data traffic from the source to destination. The arm processor attached in the source end node find the route to the destination without an attacker node. The proposed architecture for detecting and mitigating the attacker node in IoT network depicted in Fig 3. The node represented with green color are authorized node and red color are adversary node. The source node 1 wants to send data to the destination node 8, the possible paths from source to destination identified and based on the regression analysis, the source will find the best and short route without the attacker node.

For the proposed, regression modeling based attack detection, three algorithms such as Linear Regression (LR), Multi-Linear Regression

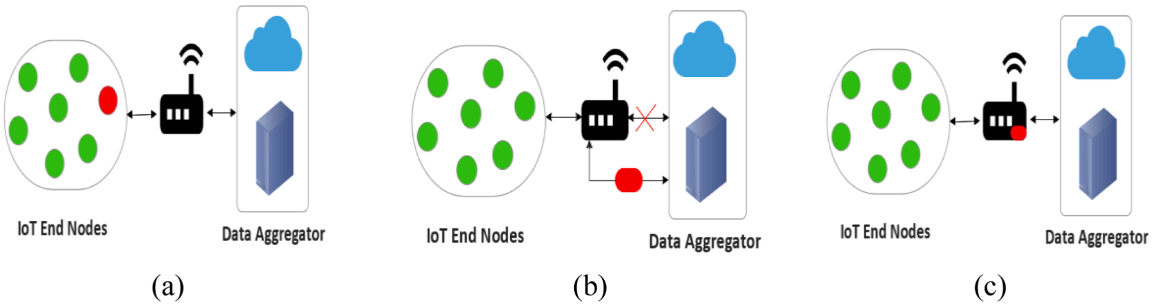

Fig 2. (a) End-point MitM (b) In-line MitM (c) In-point MitM.

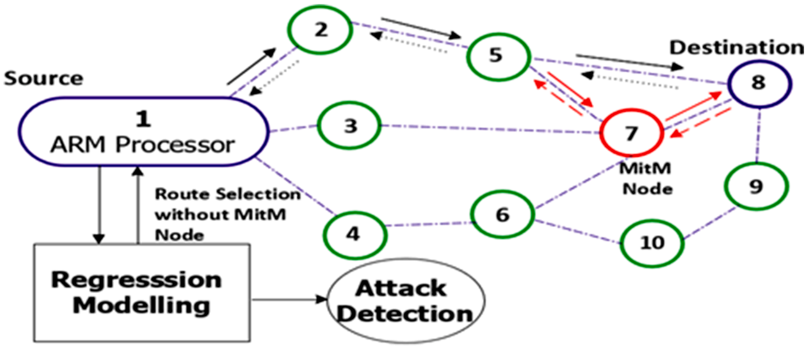

Fig 3. Proposed framework for detecting End-point MitM attack in IoT network.

(MLR) and Gaussian Process Regression (GPR) were implemented and performance were analyzed to measure the effectiveness of identifying the adversary node and selecting the route without MitM attacker node.

3.1. Linear regression

Linear Regression (LR) is a popular Machine Learning Technique used to predict the continuous data. It predicts the output or outcomes (Y) based on the given inputs (X) also called as predictors. It uses a mathematical equation for predicting the output value. It is the simple technique that assumes linear relationship between the predictor and the outcome variables for predicting continuous variable.

The mathematical equation for Linear Regression is

$$Y = a + b\sum_{i=1}^{n} X_i + e \tag{1}$$

were, Y is a dependent variable, X_i is an independent variable, a is an intercept, b is the regression coefficient, n is the set of input variables and e is the error term

The linear regression weight or coefficient calculated to minimize the error in predicted outcome values. Linear regression model takes both categorical and continuous data as predictor inputs

3.2. Multi-variate linear regression

Multi-variate Linear Regression (MLR) is an extension of simple linear regression where more than one independent predictor used for prediction of attacks. Multi-variate Regression predicts m dependent variables from the same set of independent variables. The general equation of MLR is

$$\mathrm{Y_j} = \mathrm{A_j} + \sum_{p=1}^{n}(\alpha_{pj} * X_p) + e \tag{2}$$

Where j represents the number of dependent variables indexed as $j = 1\ldots$ m, n is the number of independent variable, α_{pj} represents the regression coefficient of p (predictor) for j (outcome) and e is the error term.

3.3. Gaussian process regression

Gaussian Process Regression (GPR) is a generic supervised machine learning technique used to solve regression and probability classification problems. It accurately predicts the uncertainty measures for small data sets. It fit the appropriate function to the data among many functions by assigning probability to each of the functions and find the mean of the probability distribution among the functions to represent the most characterization of the data. This probabilistic approach gives a confidence for the predicted regression function.

For computing the predictive posterior distribution, the posterior value calculated using the data traffic by specifying the prior function space.

4. Experiments and results

This section explains the performance metrics used in the proposed work and the findings of the regression modeling illustrated.

True Positive (TP) rate refers the attacks correctly predicted as attacks, True Negative (TN) rate refers the normal traffic predicted correctly as normal, False Positive (FP) refers the wrong identification of non-attack traffic as malicious, False Negative (FN) refers the wrong identification of attack as non-attack. P' and N' refers the total number of instances predicted as attacks and normal, where P and N represents the actual number attack and non-attack observations respectively.

Accuracy estimated as the fraction of correct predictions of attacks to the total number of predictions

$$Accuracy = \frac{(TP + TN)}{(P + N)} \tag{3}$$

Precision gives the proportion of instances correctly predicted as positives among the total of positive predictions

$$Precision = \frac{TP}{p'} \tag{4}$$

Sensitivity is the recognition rate of positive instances that correctly predicted as positive

$$Sensitivity = \frac{TP}{P} \tag{5}$$

Specificity is the recognition rate of negative instances that correctly predicted as negative

$$Specificity = \frac{TN}{N} \tag{6}$$

FPR is the proportion of incorrectly classified as positive over the total number of actual negative instance

$$FPR = 1 - Specificity \tag{7}$$

FNR is the proportion of incorrectly classified as negative over the total number of actual positive instance

$$FNR = 1 - Sensitivity \tag{8}$$

FDR is the proportion of incorrectly classified as positive over the total number of predicted positive instances

$$FDR = 1 - Precision \tag{9}$$

FOR is the rate of wrongly misclassified positive as negative over the total number of negative predictions.

$$FOR = \frac{FN}{N'} \tag{10}$$

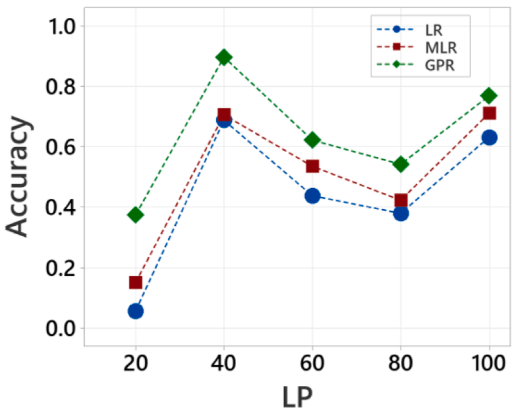

Fig 4. Accuracy Vs. Learning Percentage.

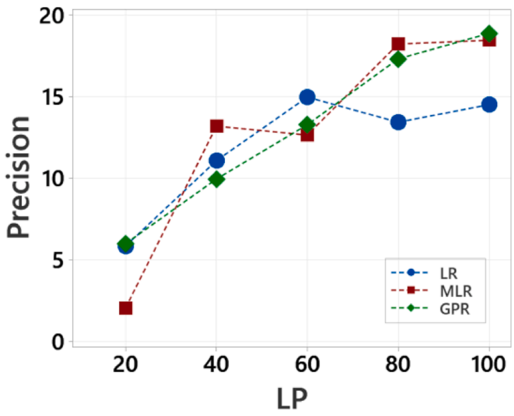

Fig 5. Precision Vs. Learning Percentage.

Performances of the Regression modeling also analyzed based on the throughput and packet lost ratio. Throughput refers the amount of data traffic successfully transmitted from source machine to the destination machine during the span of time. Packet Loss Rate used to determine the reliability of path from source to destination. It gives the ration of the number of not received data to the total number of data sent.

4.1. Performance evaluation of positive measures

Fig 4 shows the performance measures of accuracy for LR, MLR and GPR. From the figure, it clearly identified GPR produces higher accuracy rate at various learning percentage. At learning percentage of 40, GPR produces the higher accuracy rate of 89% where LR and MLR produces 68% and 70% respectively. The performance measures of precision rate shown in Fig 5. At 20%, GPR produces 5.88 precision rate whereas the rate of LR and MLR are 5.85 and 2.06 respectively. At 40%, GPR produces low precision rate compared to other two models. But GPR have constant growth in precision rate at increasing learning percentage. The evaluated values of positive metrics at different learning percentage is given in Table 3.

Figs. 6 and 7 shows the performance analysis of sensitivity and specificity rate of various classifiers LR, MLR and GPR against different learning percentage. Sensitivity rate of GPR is higher at all the learning percentage compared to LR and MLR. But LR shows the good performance measures on specificity rate. The specificity of GPR at 100%, 80%, 60%, and 40% is 0.93, 0.67, 0.68, 0.73 which is comparatively lower than LR which produces 0.95, 0.72, 0.48 respectively. But at 80% the specificity rate of GPR is higher than LR.

4.2. Performance evaluation of negative measures

Performance measures such as FDR, FNR, FOR and FPR indicates the wrongly classified instances. Figs. 8 and 9 clearly shows that GPR analysis produces lower negative measures values for FDR and FNR compared with LR and MLR at various learning percentage (LP). At 100

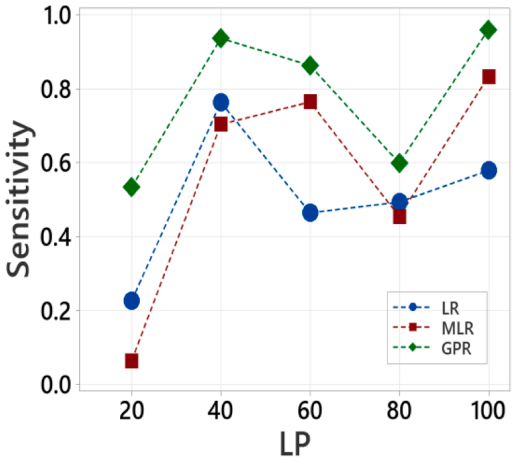

Fig 6. Sensitivity Vs. Learning Percentage.

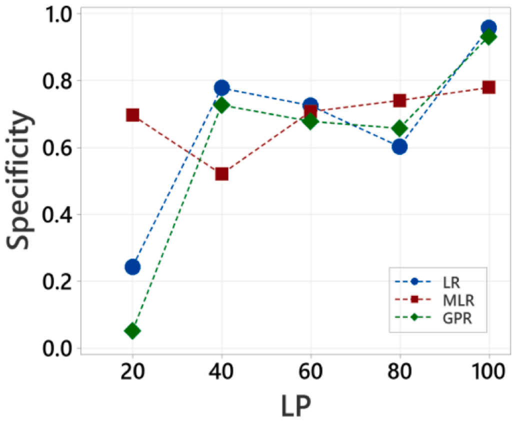

Fig 7. Specificity Vs. Learning Percentage.

Table 3
Positive Performance Analysis of LR, MLR and GPR.

LP	Accuracy			Precision			Sensitivity			Specificity		
	LR	MLR	GPR	LR	MLR	GPR	LR	MLR	GPR	LR	MLR	GPR
20	0.057298	0.151179	0.375017	5.85384	2.05085	5.99454	0.226576	0.064022	0.533979	0.243113	0.696026	0.051063
40	0.688349	0.706392	0.897731	11.0794	13.1923	9.95252	0.764415	0.704343	0.937555	0.777194	0.51997	0.726468
60	0.438495	0.535978	0.622598	14.9672	12.6433	13.2772	0.464808	0.765158	0.864107	0.724882	0.706781	0.677764
80	0.379988	0.423302	0.542437	13.4329	18.2215	17.306	0.493805	0.454935	0.599813	0.602517	0.740187	0.656897
100	0.631947	0.711363	0.769125	14.5038	18.4477	18.8699	0.579355	0.833768	0.960978	0.956183	0.778642	0.930805

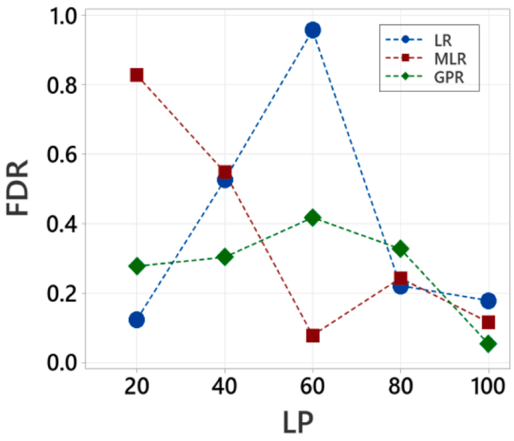

Fig 8. FDR Vs Learning Percentage.

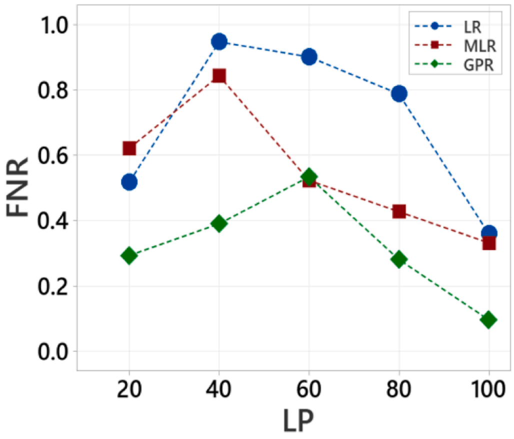

Fig 9. FDR Vs Learning Percentage.

learning percentage, the FDR of GPR is 0.05, which is very low compared with LR and MLR of 0.18 and0.12 respectively. Similarly, the rate of FNR is also low at 100% in GPR. The evaluated values of negative metrics at different learning percentage are given in Table 4.

False Omission Rate of GPR produces lower value at all learning percentage than other two classifiers, LR and MLR as shown in Fig. 10. Analysis of FPR presented in Fig. 11 at 20% and 40% GPR produces Lower Positive Rate. But at 60% FPR of GPR is 0.72, comparably higher than LR and MLR, that is 0.64 and 0.53 respectively. At 80% and 100%, it is slightly high compared to others. Overall GPR produces the lower values for negative measures at most of the learning percentages.

4.3. *Analysis of packet loss ratio*

The performance based on Packet loss ratio is explained under varied attack rate to 5%, 10%, 15%, and 20%. From the Fig. 6(a), it is observed that GPR produces the lower packet loss ratio compared to LR and MLR. At the attack rate of 5%, the packet loss ratio of GPR is 8.42% whereas it is 9.5% and 12.43% for LR and GPR. At the attack rate of 10%, the packet loss ratio of GPR is 12.98% whereas it is 14.36% and 15.81% for LR and GPR. At the attack rate of 15%, the packet loss ratio of GPR is 17% whereas it is 18.34% and 19.35% for LR and GPR. At 20%, the packet loss ratio of GPR is 2.17% which is low among the different attack rates whereas it is 3.84% and 7.64% for LR and GPR. Thus GPR produces less packet loss and proves its efficiency.

4.4. *Analysis of throughput*

Fig. 6(b) shows the throughput analysis of LR, MLR and GPR over varied attack rate. It is observed that GPR produces higher throughput rate at all attack rates expect at 20%, where LR produces slightly higher rate of 0.44% and GPR produces 0.42%. Also it is noted that MLR produces lower throughput compared to LR and GPR. At attack rate of 10%, GPR produces the maximum throughput of 0.94% whereas LR and MLR attains 0.91% and 0.49%. From the observed values, it is cleared at GPR delivers more number of packets successively; hence GPR makes an attack free communication compared to LR and MLR.

5. Conclusion

This paper provides solution to detect and mitigate MitM attack in IoT network. For adversary node detection, this work proposed Regression modeling to find the attack-free route from source to the destination. Three machine learning regression techiques LR, MLR and GPR are implemented and perfomance of each techniques are analyzed based on various metrics. Packet loss ratio and throughput of each classifier is also estimated and analyzed. Results shows that among the three, the performance of Gaussian Process Regression techniques is more efficient in detecting MitM attacks.

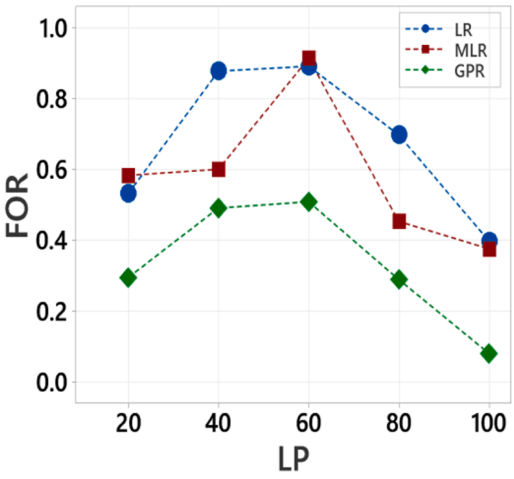

Fig 10. FOR Vs Learning Percentage.

Table 4
Negative Performance Analysis of LR, MLR and GPR.

LP	FDR			FNR			FOR			FPR		
	LR	MLR	GPR	LR	MLR	GPR	LR	MLR	GPR	LR	MLR	GPR
20	0.12454	0.828913	0.277823	0.518309	0.621861	0.293311	0.532407	0.583485	0.295174	0.431038	0.625911	0.368554
40	0.526756	0.548653	0.3041	0.947613	0.844052	0.390485	0.878338	0.600977	0.491497	0.583299	0.568593	0.120073
60	0.958168	0.078614	0.418037	0.901922	0.523354	0.534068	0.89218	0.914078	0.508972	0.882654	0.423039	0.54443
80	0.221708	0.243596	0.327547	0.788383	0.427654	0.281245	0.697995	0.453472	0.289239	0.586345	0.575348	0.626803
100	0.178673	0.116629	0.054586	0.360552	0.331981	0.096269	0.397971	0.376074	0.080464	0.646709	0.536413	0.712903

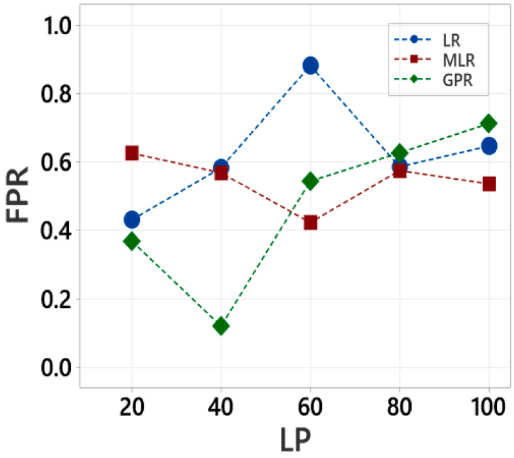

Fig 11. FPR Vs Learning Percentage.

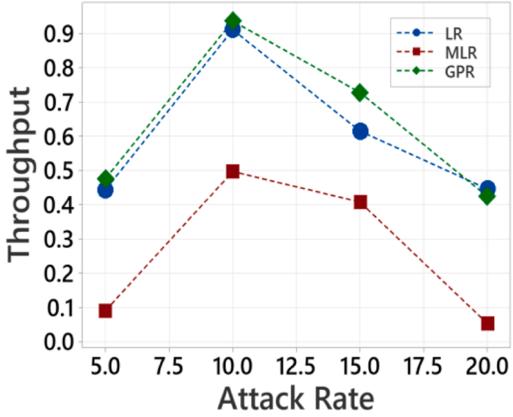

Fig 12. Performance of Throughput.

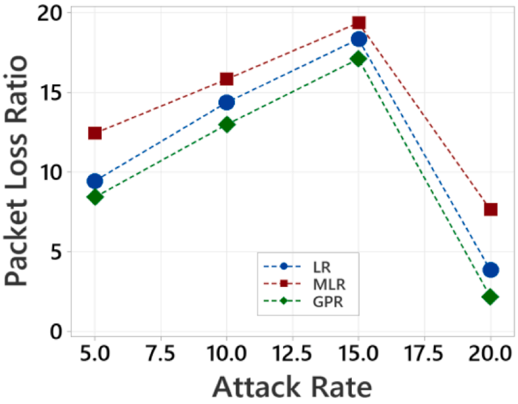

Fig 13. Performance of Packet Loss Ratio.

Declaration of Competing Interest

None.

References

[1] Hatzivasilis G, Soultatos O, Chatziadam P, Fysarakis K, Askoxylakis I, Ioannidis S, Alexandris G, Katos V, Spanoudakis G. WARDOG: awareness Detection Watchdog for Botnet Infection on the Host Device. IEEE TRANS SUSTAINABLE COMPUT 2021;6. VOLNO. 1, JANUARY-MARCH.

[2] Heartfield Ryan, Loukas George. Anatolij Bezemskij, and Emmanouil Panaousis, “self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. IEEE Trans Inf Forensics Secur 2021;16. VOL.

[3] Meng Weizhi, Li Wenjuan, Zhu Liqiu. Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. IEEE Trans Eng Manage 2020;67. VOLNO. 4, NOVEMBER.

[4] Mourad A, Tout H, Abdel Wahab O, Otrok H, Dbouk T. Ad-hoc vehicular fog enabling cooperative low-latency intrusion detection. IEEE INTERNET OF THINGS J 2020. VOL., NO., APRIL.

[5] Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, And Kim-Kwang Raymond Choo, “A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks”, IEEE transaction on Emerging topics in Computing, VOLUME 7, NO. 2, APRIL-JUNE 2019.

[6] Laisen Nie, Yixuan Wu, Xiaojie Wang, Lei Guo, Guoyin Wang, Xinbo Gao, and Shengtao Li, “Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial network-based approach”, IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS.

[7] S.Prabavathy KSundarakantham, Shalinie SMercy. Design of cognitive fog computing for intrusion detection in internet of things. J COMMUN NETWORKS 2018;20(3). VOLNOJUNE.

[8] Parminder Singh,Avinash Kaur, Gagangeet Singh Aujla, Ranbir Singh Batth, and Salil Kanhere, “DaaS: dew computing as a service for intelligent intrusion detection in edge-of-things ecosystem”, IEEE INTERNET OF THINGS JOURNAL, 2020.

[9] Bighnaraj Naik, Mohammad S. Obaidat, Janmenjoy Nayak, Danilo Pelusi, Pandi Vijayakumar, and S.K. Hafizul Islam, “Intelligent secure ecosystem based on meta-heuristic and functional link neural network for edge-of-thing” doi:10.1109/TII.2019.2920831, IEEE Transactions on Industrial Informatics.

[10] Faezeh Farivar, Mohammad Sayad Haghighi, Alireza Jolfaei, and Mamoun Alazab, “Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber physical systems and industrial IoT”, doi:10.1109/TII.2019.2956474, IEEE Transactions on Industrial Informatics.

[11] Paulo Freitas de Araujo-Filho, Georges Kaddoum, Divanilson R. Campelo, Member, Aline Gondim Santos, David Macedo, and Cleber Zanchettin, “Intrusion detection for cyber-physical systems using generative adversarial networks in fog environment”, doi:10.1109/JIOT.2020.3024800, IEEE Internet of Things J.

Sivasankari Nitiynandan, born in Puducherry on 13th September 1985. She received the BCA degree in Computer Applications and MCA degree in Computer Application from Pondicherry University, India in 2005 and 2008 respectively. Currently she is working as a Teaching Fellow in Anna University, Chennai and pursuing her part-time research in VISTAS, in the field of securing Internet of Things application using Machine Learning techniques. Her areas of interest are IoT, Machine Learning, Network Security, and Wireless Sensor Network.

Dr. S. Kamalakkannan received his M.Sc Computer Science Degree from Bharathidasan University, M.Phil. Computer Science Degree from Periyar University, and Ph.D. in Computer Science from Vels Institute of Science, Technology & Advanced Studies (VISTAS) Tamil Nadu, India. He is currently working as Associate Professor, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India, which is a well-known university. He has 17 years of teaching experience in both UG and PG level. His-research interest includes Data Mining, Big Data Analytics, and Block Chain Technology. He has produced five M.Phil. Research scholars. He has published more than 35 research articles in various international journals such as Scopus and UGC referred journal. He serves as an Examiner in various Universities and Colleges. He received Best Young Scientist award and Best Faculty award.