Machine Learning-Based Recommendation Trust Model for Machine-to-Machine Communication

Elvin Eziama[1],Luz M.S Jaimes[2], Agajo James[3],Kenneth Sorle Nwizege[4],Ali Balador[5] and Kemal Tepe[6]
[1]Windsor University, Canada, eziama@uwindsor.ca
[2]Grupo Ciencias Computacionales - Universidad de Pamplona, Colombia, lsantosj@icmc.usp.br
[3] Computer Engineering, Federal University of Technology, Mina Nigeria
[4]Ken Saro-Wiwa Polytechnic, Bori, Nigeria, s.k.nwizege@ieee.org
[5]Mälardalen University, Sweden, ali.balador@mdh.se
[6]Windsor University, Canada, ktepe@uwindsor.ca

Abstract— **The Machine Type Communication Devices (MTCDs) are usually based on Internet Protocol (IP), which can cause billions of connected objects to be part of the Internet. The enormous amount of data coming from these devices are quite heterogeneous in nature, which can lead to security issues, such as injection attacks, ballot stuffing, and bad mouthing. Consequently, this work considers machine learning trust evaluation as an effective and accurate option for solving the issues associate with security threats. In this paper, a comparative analysis is carried out with five different machine learning approaches: Naive Bayes (NB), Decision Tree (DT), Linear and Radial Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Random Forest (RF). As a critical element of the research, the recommendations consider different Machine-to-Machine (M2M) communication nodes with regard to their ability to identify malicious and honest information. To validate the performances of these models, two trust computation measures were used: Receiver Operating Characteristics (ROCs), Precision and Recall. The malicious data was formulated in Matlab. A scenario was created where 50% of the information were modified to be malicious. The malicious nodes were varied in the ranges of 10%, 20%, 30%, 40%, and the results were carefully analyzed.**

Keywords - **Machine Type Communication Devices, Machine-to-Machine(M2M), Internet of Vehicles(IoVs), Internet of Things(IoTs), Supervisory Control and Data Supervisory Acquisition (SCADA)**

I. INTRODUCTION

Machine-to-Machine Communication (M2MC) is a new technology where a large number of intelligent devices can autonomously communicate with each other and make collaborative decisions without direct human intervention [1]. This is a cost effective approach that utilizes effective time management. The communication has its origin in the Supervisory Control and Data Supervisory Acquisition (SCADA) systems, where sensors and other devices that are connected through wired or radio frequency networks are used with computers to monitor and control industrial processes.

It is important to note the integration of varieties and the range of M2M applications which are outlined in Fig I. Fig I, illustrates the functionality of the devices and other requirements as key features of M2MC and its future markets. The inclusion of these attributes in M2MC, we can understand the flexibility in M2M architecture and how it can be developed to integrate the present and future technologies.To achieve this promising technology, it is

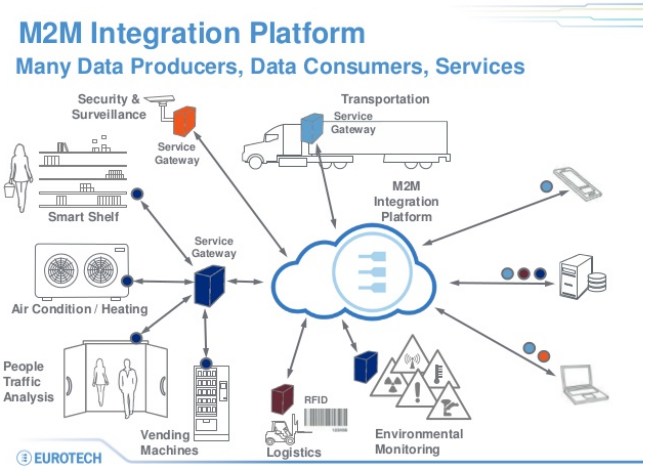


Fig. 1. M2M Structure (EurOtech)

Establishing a reliable incorporation of the M2M communication in the Internet of Things (IOTs) settings, such as Internet of Vehicles (IOVs) and Vehicular Ad-Hoc Networks (VANETs), will envisage a future in which digital and physical things or objects (e.g., smart phones, TVs, cars) can be connected by means of suitable information and communication technologies to enable a range of applications and services [2], [3], such as transportation safety, enhancement of traffic throughput, efficient resource allocation, and convenient environment. In addition, the robust nature of M2M communication will provide efficient distributive collection and dissemination of information among device/nodes in a given network [1], [4], [5].

Consequently,when reliable M2MC is established in a network, it can significantly improve the performance of devices/nodes that maintain good connections with neighbors,

978-1-5386-7568-7/18/$31.00 ©2018 IEEE

allowing for faster decisions and rendering update of their status. For example, in vehicular networks, they can improve emergency responses in instances of vehicular accidents.

However, during information exchange, some nodes may decide to communicate malicious reports for their personal interests. These attacks in MTCDs environments are of concern in communication fields, such as VANETs and IOVs, when considering their vulnerable nature. This situation calls for a more reliable approach to checkmate the bad behaviors of adversary nodes. This paper proposes the application of machine learning trust models as better approaches in detecting the behaviors of adversary nodes.

Thus, the major contribution of this paper is to provide performance comparison indices of different machine learning trust models in the detection of attacks of different adversary in M2M communication networks.

The rest of the paper is organized as follows. Section II sheds light on the different attack mechanisms in M2M communication systems and the notion of trust. Section III gives an overview of the related works in the literature on M2M systems, security issues, and possible solutions. Section IV deliberates on the attack formulation, as determined in this paper, and proposes detection models. Section V discusses the evaluation metrics and simulation results in this paper. Finally, section VI discusses the conclusion and references respectively.

II. ATTACKS MECHANISMS AND NOTION OF TRUST

This section discuss the different attack mechanism and different categories of trust.

A. ATTACK MECHANISM

The ability of the trust evaluation protocol to detect malicious participant in the M2M communication devices is of concern in their applications in a real-time situation. Some peers of nodes may have special and conflicting interest in their recommendation process [1]. These malicious agents can collude to dominate the network. This dominance can enable them to be recommended during voting scheme when considering Entity Centric Trust (ECT). The recommendation of a given node by another node can be altered for popularity gain by a malicious node in the voting scheme [1]. This can come in form of bad mouthing or ballot stuffing, self-promotion, on-and-off and opportunistic attacks. Bad mouthing and ballot stuffing are basically attacks based on self-interest, while on-and-off attacks are often used by adversaries to evade detection.

There are five common forms of Trust Related Attacks on M2M communication:

1) Self Promotion Attacks (SPA) This is a situation whereby a malicious node promotes itself so as to be selected as a service provider in a voting scheme but ends up relying on dishonest information in the network.
2) Bad Mouthing Attack (BMA) Malicious node gives a bad recommendation of an honest node just to ruin the reputation of the node from being selected as a service provider. Malicious nodes can collude to launch a collusion attack on the honest node in this contest.
3) Ballot Stuffing Attack: In this regard, malicious nodes end up promoting the interest of a dishonest node, so as to be selected in a voting scheme in a network.
4) White-Washing Attack : This attack mechanism comes in the form of on-and-off process, whereby nodes enter and leave the network so that they will not be labeled as malicious nodes. When the reputation of a node drastically deteriorates, it may decide to leave the network only to rejoin the network thereafter. This is done to regain reputation and continuation of bad mouthing and ballot stuffing attack in the network.
5) Opportunistic Attack malicious agent/node tends to provide good service to the network when it senses that its reputation is drastically going low. However, if the node ends up regaining good reputation it will collude with another malicious node to provide a malicious report to service requester in the network.

B. THE NOTION OF TRUST

Trust can be defined as the subject belief of peers of nodes belonging to the same geographical location [6]. It can also be defined as the expectation from a given agent for providing reliable information.

This mechanism can be represented in many forms: such as in binary notion of ”1” and ”0”, multilevel form as level 1, 2, probabilistic form with values ranging from 0 to 1 and so on [6].

The idea of trust is gaining importance in different areas of applications, such as VANETs, IoVs and in M2M communications in general. The mechanism involves nodes/devices learning about events from their neighbors.

This concept can be grouped into three categories, namely:

- Entity Centric Trust (ECT)
  Here, trust is assigned on the entities or nodes in a given networks.
- Data Centric Trust (DCT)
  Trust is assigned on the information given by the entities, order than the entities or nodes themselves.
- Hybrid Trust (HT) This is simply the combination of both ECT and DCT

III. RELATED WORKS

In M2M communication different applications will be fully realized if security as a factor is properly addressed on time [7]. There is an urgent requirement for security procedures and mechanisms, although different characteristics of M2MC systems can create some design challenges in the establishment of sound security mechanism. Many of the state-of-the-art security mechanisms have been applied in M2M with respect to VANETs, yet, the security structures in M2M paradigm still require new approaches to security. The Work in [3], shows that M2M communications have been recently introduced in smart grid and vehicular networking environments. It shows that the concepts can improve electrical vehicular networking while offering two-way communication between Electric Vehicles (EVs) and Electric Vehicle Supply Equipment (EVSEs). In this paper, study is made on the impacts of a very large number of connected EVs when attempting to use the random access in LTE-Advanced to communicate with the grid. In addition, they proposed an effective solution for avoiding congestion on the random access channel of LTE-Advanced for massive EV-2-EVSE communications, which differentiates between two classes of service of EVs communications, giving priority to charging demands over other types of messages lower priority messages(promotions, subscriptions, mechanical checks, etc.).

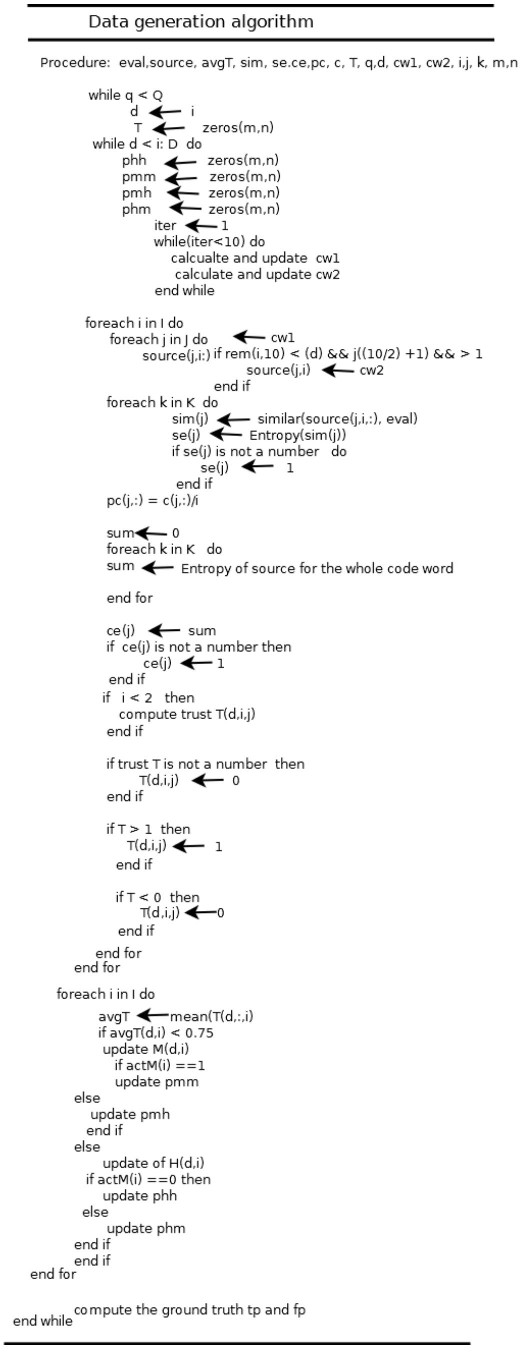
Paper [8], carefully investigated a Vehicular M2M (VM2M) overlay network over random access channel (RACH) in LTE that aims to emulate the control channel (CCH) of VANETs. The work describes how VM2M overlay is implemented over a dedicated subset of preamble codes at the physical layer, and uses a medium access control (MAC) layer modeled as IEEE 802.15.4 carrier sense multiple access (CSMA/CA) mechanism. They evaluated the performance and interaction of regular LTE (H2H) traffic and VM2M traffic, and the impact of RACH resource configuration and preamble format (PF) in large cells. It was discovered that the format $PF = 2$ is capable but not ideal for handling large amount of CCH traffic due to repeated preamble transmissions in H2H layer; better results may be obtained if the frequency of RACH sub-frame allocation for CCH is increased, or a larger number of preambles is used at the physical layer of CCH.

IV. ATTACK FORMULATION AND DETECTION MODELS

This section discusses how attack is formulated in this paper and the different detection mechanisms as applied in the M2M communication networks

A. Attack Formulation

The attack formulation algorithm of Fig 2 is well described in [1]. The paper formulates a robust algorithm for on-and-off attack and false feed back among peers (bad mouthing and ballot stuffing attacks) in the network with the integration of consistency in its modeling. In the paper, network of connected vehicles/nodes are generated from the Matlab simulation. In this regard, nodes transmit their opinions in a scheduled broadcast in the form of recommendation to q of their neighboring nodes. Nodes may decide to report malicious information for their personal interest. Adversary nodes can send modified information in the form of recommendation with the probability of p. Furthermore, in the formulation, in [1] error probability of 0.04 is assigned for the misjudgment of honest nodes. The simulation work presents 50% of the nodes to be malicious. In this paper, different percentages of the malicious nodes are simulated and the data generated with the output result of True Positive Rate (TPR) and False Positive Rate (FPR) are gathered.The ground truths of TPR and FPR derived from [1], serve as the input data to this paper's comparison analysis of different machine learning models.



```
Data generation algorithm

Procedure:  eval,source, avgT, sim, se.ce,pc, c, T, q,d, cw1, cw2, i,j, k, m,n

while q < Q
        d ←  i
        T ←   zeros(m,n)
 while d < i: D  do
       phh  ←  zeros(m,n)
       pmm  ←  zeros(m,n)
       pmh  ←  zeros(m,n)
       phm  ←  zeros(m,n)
            iter ← 1
            while(iter<10) do
               calcualte and update  cw1
                calculate and update cw2
            end while

foreach i in I do
     foreach j in J do     ← cw1
          source(j,i:) if rem(i,10) < (d) && j((10/2) +1) && > 1
                         source(j,i)  ← cw2
                     end if
     foreach k in K  do
               sim(j) ← similar(source(j,i,:), eval)
               se(j) ← Entropy(sim(j))
               if se(j) is not a number   do
                     se(j)  ←   1
                end if
     pc(j,:) = c(j,:)/i

     sum← 0
     foreach k in K   do
     sum  ← Entropy of source for the whole code word

     end for

     ce(j)  ←  sum
     if  ce(j) is not a number then
            ce(j) ← 1
      end if
    if   i < 2   then
       compute trust T(d,i,j)
     end if

     if trust T is not a number  then
           T(d,i,j)  ←  0
     end if

     if T > 1  then
        T(d,i,j) ←  1
       end if

       if T < 0  then
           T(d,i,j) ←0
        end if
   end for
 end for

foreach i in I do
       avgT ←mean(T(d,:,i)
       if avgT(d,i) < 0.75
        update M(d,i)
          if actM(i) ==1
          update pmm
    else
       update pmh
      end if
    else
        update of H(d,i)
      if actM(i) ==0 then
        update phh
     else
         update phm
    end if
    end if
end for

         compute the ground truth tp and fp
end while
```

Fig. 2.   Data Generation algorithm

B. Machine Learning Detection Models (MLDM)

In this section, brief discussions are made on the different MLDM used in this paper.

1) Naive Bayes(NB): This is simply a probabilistic model that uses Bayes theorem with the assumption of independent attributes given by the class variable values [9]. This paper presents a detailed explanation of the mathematical representation of the trust computation process while using *NB* model in the attack detection in vehicular communication systems. The system is composed of ground truths from [1], represented as D components and a reliability measure of Bernoulli random variables, $X_i \sim Ber(x \mid p_j)$, with a value of 0 or 1, $\{0,1\}$.
$X_i = 0$ represents malicious node
$X_i = 1$ represents honest node
The model is represented as a classification process using total probability theorem below:

$$p(X_i \mid D) = \frac{P(D \mid Xi)p(X_i)}{\sum_{X\in(0,1)}[p(D \mid Xi)p(X_i)]} \tag{1}$$

2) Logistic Regression (LR): The LR model is capable of accommodating the pattern of behaviors of vehicular nodes in a given system as a result of operational behaviors of the vehicular nodes, the environmental variation changes and so on.

The correlations between the regressor variables help to compute the trustworthiness of the information sent by the nodes [10].

The LR model is generalized as a binary classification process. The output label X_i, represents malicious and honest nodes as reflected in NB's section. The label is represented mathematically as: $X_i \in \{0,1\}$. To have a better binary classification, the Gaussian distribution of $X_{0,1}$ is replaced with Bernoulli distribution [11]. The posterior probability of the model is represented as follows:

$$P(X_i \mid D, \beta) = Ber(X_i \mid \mu(x)) \tag{2}$$

Given that $\mu(x) = [X_{0,1} \mid D]$,
where
$\mu(x) = Sigma\left(\beta^T X\right)$
and $Sigma\left(\beta^T X\right) \triangleq \frac{1}{1+e^{-}\beta^T X}$

The output of the model is interpreted as a probability with the help of the sigmoid function $Sigma\left(\beta^T X\right)$.
Thus,

$$P\left(X_{(0,1)} \mid D, \beta\right) = Ber\left(X_{0,1} \mid Sigma\left(\beta^T X\right)\right) \tag{3}$$

where $X_{(0,1)}$ denotes a set of evidence, while D is the operational and the environmental variables, β is the latent variable between the $X_{(0,1)}$ and D to be estimated.

3) Support Vector Machine (SVM): Basically, the output of the model being y_i is represented as follows:

$$y_i = \begin{cases} 1 & \textit{honest node} \\ -1 & \textit{malicious node} \end{cases} \tag{4}$$

Given that x_i in each observation and b the threshold, the hyper-plane is represented as $y_i(wx_i + b)$. Furthermore, SVM maximizes the margin between classes of honest and malicious nodes in the network such that $(wx_i + b) = 0$.
Thus:
the training observation satisfies the following:
$wx + b \geq -1$ denotes malicious nodes and $wx + b \leq -1$ for all honest nodes.

4) K-Nearest Neighbors (KNN): The model is an instance based approach which works on the basis of similarities between nodes in the network. The similarities can be measured with Euclidean distance, Manhattan distance function and so on. This paper considers Euclidean distance for the KNN trust model. Thus, the Euclidean distance between two input vectors X_i, X_j to the system to be $D_{ij} = \sqrt{\sum_{k=1}^{n}\left(X_{ik} - X_{jk}\right)^2}$ $k = 1, 2, ...n$.
For every message point in the messages, the Euclidean distance between the current point and the input message point is computed. Thus, K with the lowest distance to the input message point is selected, as such the majority class is found and the model returns the majority class to be the classification to the input point. This iterative measure, enables trust computation and possible detection of unwanted information in the network by way of classification.

5) Random Forest (RF): The RF helps in aggregating weak models in trust computation. This in other words, has to do with the ensemble of classification or regression trees or nodes in this paper [11].
Mathematically, RF can be expressed as follows:
$R = \{t_1, t_2, ..., t_N\}$, when each of the trees t is constructing, it learns a function $F : X \to C_{(0,1)}$
Possible estimation is done on the output class $C_{(0,1)}$, which comprises of malicious and honest information. Thus, given that the output label is $C_{0,1}$, we denote 0 and 1 as malicious and honest information respectively. The probability of estimation of the output variables can be expressed as follows: $P\left(C_{(0,1)} \mid X\right) = \frac{1}{N}\sum_{i=1}^{N} P_i\left(C_{(0,1)} \mid X\right)$. An adaptive threshold is automated by the model in determining the best estimation that can accurately classify both the malicious and honest information.

V. EVALUATION METRICS AND SIMULATION RESULTS

A. Model simulation

The software tool chain used in the implementation of the different machine learning models in this paper consists of Jupyter notebook development environment and Sci-kit learn. The algorithm used in [1], enables the user to formulate the features such as coordinate distance among the nodes, the number of messages, the time variation of the nodes opinions, and frequency as inputs to the machine learning analysis. The training and testing phase of the model analysis involves 70% and 30% percentages of the nodes information.

B. Results and Evaluations

In this study, two prominent metrics for model performance evaluation are used to evaluate the different machine learning trust models which are Receiver Operation Characteristics (ROC), and Precision-Recall curve. These evaluation metrics are calculated using confusion metrics as follows:

- True Positive (TP): if a malicious information is classified by the model as malicious, then the result is accepted as TP
- False Positive (FP): if an honest information is classified by the model as malicious, then the result is taken as FP.
- True Negative TN: in this case, when a a malicious information is classified by the model as honest, result is taken as TN.
- False Negative FN: if an honest information is classified by the model as honest instance, the result is accepted as FN

1) A Receiver Operation Characteristics (ROC): TPR is the number of positive data points that are correctly predicted as positives. TPR known also as sensitivity or recall is defined as follows:

$$TPR = \frac{TP}{TP+FN} \tag{5}$$

While FPR is the proportion of the negative message points mistakenly predicted to be positive for all the negative message points. This can be demonstrated mathematically as follows:

$$FPR = \frac{FP}{FP+TN} \tag{6}$$

Based on the simulation results, Figs 2-4 show the performances of different trust computation models for the classification carried out on 20%, 30% and 40% percentages of malicious information sent by the adversary nodes respectively. Considering the ROC performance scores as indicated in the three tables, DT and RF show a superior performance over all other models in presenting a sound quality prediction. The two have an area under ROC curve score of 1 as shown in the three tables. LT and KNN and SVM-linear relatively performed well while SVM-rbf shows the least performance among the seven machine learning trust models evaluated in the specified percentages of modified information.

2) Precision and Recall Curve: This can be seen as the measure of the relevance of results, while recall indicates the number of genuinely returned relevant results. The higher the two metrics, the more accurate the performance of the model. Individually, the two metrics do not give a complete hint of the classifier performance. They are merged together to form Precision-Recall Curve, which presents a more meaningful performance metrics. Figures 6-8, depict PRC, all the LR, DT, RF and NB in the respective percentages of maliciously modified information, show very good scores of 100% in the three PRC plots as indicated in Tables 1-3. KNN and SVM linear present average performance in the three plots as shown in their scores in the three tables respectively. Again, SVM-rbf remains insensitive to the behaviors of the malicious nodes by having a result of 0.00 % in both precision and recall process as reflected in the three tables of the of maliciously modified information.

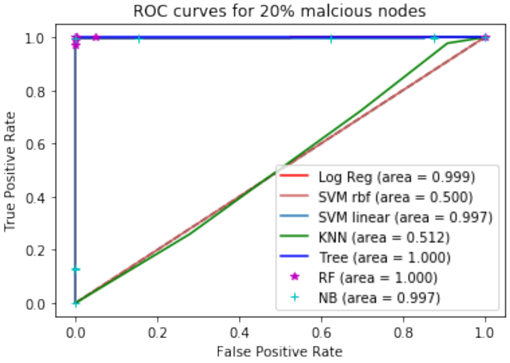


Fig. 3. Comparison of RoC curves of different Machine Learning Models where 20% of the messages are Modified

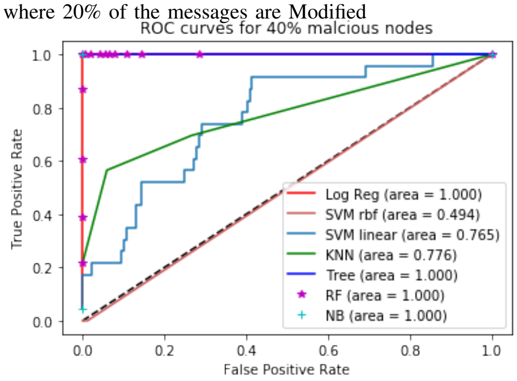


Fig. 4. Comparison of RoC curves of different Machine Learning Models where 30% of the Messages are Modified

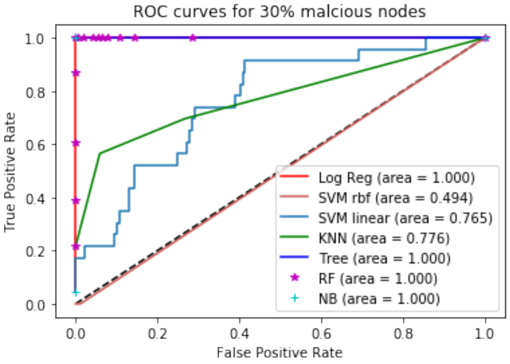


Fig. 5. Comparison of RoC Curves of Different Machine Learning Models with 40% of the Messages Modified

TABLE I

ACCURACY RESULT OF 40% OF MALICIOUS MESSAGES

Model Name	AUC	Precision	Recall
LR	1.000	1.000	1.000
SVM rbf	0.494	0.000	0.000
SVM linear	0.765	0.043	0.56
KNN	0.765	0.560	0.560
DT	1.000	1.000	1.000
RF	1.000	1.000	1.000
NB	1.000	1.000	1.000

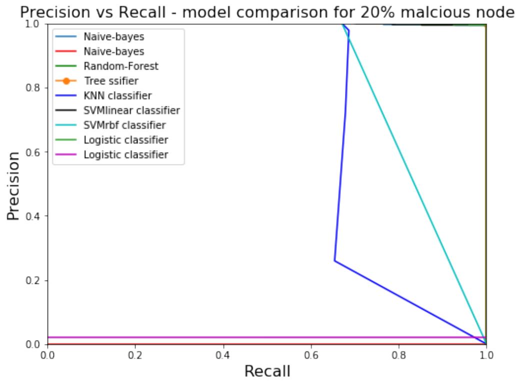


Fig. 6. Precision-Recall Curves with 20% of the Messages are Modified

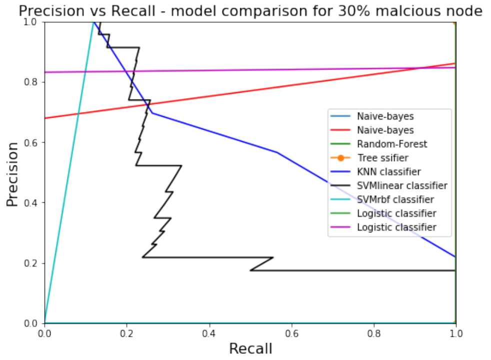


Fig. 7. Precision-Recall Curves where 30% of the Messages are Modified

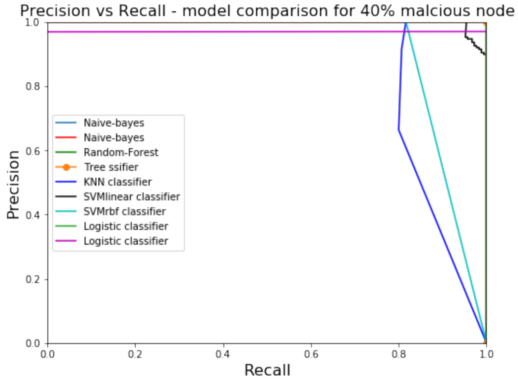


Fig. 8. Precision-Recall Curves where 40% of the Messages are Modified

TABLE II

ACCURACY RESULT OF 20% OF MALICIOUS MESSAGES

Model Name	AUC	Precision	Recall
LR	1.000	1.000	1.000
SVM rbf	0.494	0.000	0.000
SVM linear	0.765	1.000	0.040
KNN	0.765	0.560	0.560
DT	1.000	1.000	1.000
RF	1.000	1.000	1.000
NB	1.000	1.000	1.000

TABLE III

ACCURACY RESULT OF 30% OF MALICIOUS MESSAGES

Model Name	AUC	Precision	Recall
LR	0.999	1.000	1.000
SVM rbf	0.500	0.810	1.000
SVM linear	0.997	0.930	1.000
KNN	0.512	0.810	0.910
DT	1.000	1.000	1.000
RF	1.000	1.000	1.000
NB	0.997	1.000	1.000

VI. CONCLUSION

The essence of M2M communication is to maintain interoperability, scalable connection, and provision of reliable information among the enormous heterogeneous devices or nodes. However, as explained in this paper, some of these nodes may decide to communicate wrong reports for their personal interest. This issue of malicious behaviors of nodes in the communication network remains a very big challenge in the communication fields. This paper proposes the application of machine learning trust models in evaluating the trust from the information provide by the nodes in the network. Effort is made in this paper to investigate the comparative performances of different machine learning trust model such as LR, NB,SVM-rbf , SVM-linear, KNN, DT, RF in M2M communications.Based on the overall performance in both ROC and PRC with respect to the different percentages of malicious nodes, the paper recommends the use of RF in M2M communication.
Future work on this will be on the comparison of the attack formulation algorithm used in this paper with other existing ones. Additionally, comparing different deep learning models on the different attacks in network layer.

REFERENCES

[1] S. Ahmed and K. Tepe, "Entropy-based recommendation trust model for machine to machine communications," in *Ad Hoc Networks*. Springer, 2017, pp. 297–305.

[2] R. Cai, Z. Zhang, A. K. Tung, C. Dai, and Z. Hao, "A general framework of hierarchical clustering and its applications," *Information Sciences*, vol. 272, pp. 29–48, 2014.

[3] J. Rezgui and S. Cherkaoui, "An m2m access management scheme for electrical vehicles," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[4] Y. Cao, T. Jiang, and Z. Han, "A survey of emerging m2m systems: Context, task, and objective." *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1246–1258, 2016.

[5] A. E. Mostafa and Y. Gadallah, "Uniqueness-based resource allocation for m2m communications in narrowband iot networks," in *Vehicular Technology Conference (VTC-Fall), 2017 IEEE 86th*. IEEE, 2017, pp. 1–5.

[6] S. Ahmed, "Trust establishment and management in adhoc networks," 2016.

[7] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (d2d) communication: A review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[8] N. Khan, J. Mišić, and V. B. Mišić, "Vm2m: An overlay network to support vehicular traffic over lte," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*. IEEE, 2016, pp. 13–18.

[9] D. A. Effendy, K. Kusrini, and S. Sudarmawan, "Classification of intrusion detection system (ids) based on computer network," in *Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017 2nd International conferences on*. IEEE, 2017, pp. 90–94.

[10] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "Logittrust: A logit regression-based trust model for mobile ad hoc networks," in *6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA*, 2014, pp. 1–10.

[11] C. Robert, "Machine learning, a probabilistic perspective," 2014.