Article

A Machine Learning Based Intrusion Detection System for Mobile Internet of Things

Amar Amouri ¹, Vishwa T. Alaparthi ² and Salvatore D. Morgera ^{1,*}

¹ Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA; aamouri@mail.usf.edu

² Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA; vishwa.alaparthi@duke.edu

* Correspondence: sdmorgera@usf.edu; Tel.: +1-813-974-1004

Received: 10 October 2019; Accepted: 11 January 2020; Published: 14 January 2020

Abstract: Intrusion detection systems play a pivotal role in detecting malicious activities that denigrate the performance of the network. Mobile adhoc networks (MANETs) and wireless sensor networks (WSNs) are a form of wireless network that can transfer data without any need of infrastructure for their operation. A more novel paradigm of networking, namely Internet of Things (IoT) has emerged recently which can be considered as a superset to the afore mentioned paradigms. Their distributed nature and the limited resources available, present a considerable challenge for providing security to these networks. The need for an intrusion detection system (IDS) that can acclimate with such challenges is of extreme significance. Previously, we proposed a cross layer-based IDS with two layers of detection. It uses a heuristic approach which is based on the variability of the correctly classified instances (CCIs), which we refer to as the accumulated measure of fluctuation (AMoF). The current, proposed IDS is composed of two stages; stage one collects data through dedicated sniffers (DSs) and generates the CCI which is sent in a periodic fashion to the super node (SN), and in stage two the SN performs the linear regression process for the collected CCIs from different DSs in order to differentiate the benign from the malicious nodes. In this work, the detection characterization is presented for different extreme scenarios in the network, pertaining to the power level and node velocity for two different mobility models: Random way point (RWP), and Gauss Markov (GM). Malicious activity used in the work are the blackhole and the distributed denial of service (DDoS) attacks. Detection rates are in excess of 98% for high power/node velocity scenarios while they drop to around 90% for low power/node velocity scenarios.

Keywords: intrusion detection systems; WSN; IoT; random forest; AMoF; linear regression

1. Introduction

Mobile adhoc networks (MANETs), wireless sensor networks (WSNs), and Internet of Things (IoT) are a class of networks that deploy low resources nodes and the nodes that require rapid deployment. The goal is to develop an intrusion detection system (IDS) capable of dealing with such constraints. These IoT devices not only help in transmitting and receiving data, but also connect various devices to the Internet. These devices can be mobile or stationary depending on the application they are supposed to be used for. MANETs and mobile WSNs are the type of IoT networks, we are attempting to secure in this work. Machine learning and artificial intelligence-based IDSs were studied extensively during the last decade. Various machine algorithms were explored such as: Neural networks [1] and its newer version, deep learning [2], support vector machines (SVM) [3], decision trees [4], k-NN clustering [5], and Naïve Bayes [6]. However, a study presented by [7] shows several advantages for using random forest when it comes to the complexity, accuracy, and memory usage. The rationale for

using random forest as a core algorithm in our previous cross layer-based IDS is its suitability for the resource restrictions inherent in the afore mentioned networks [8].

Apart from machine learning there are other techniques which have been employed to build an intrusion detection system. A broader classification of these techniques, segregates IDSs as anomaly-based IDSs, signature based, and specification based IDSs. Markov models and hidden Markov models [9] have been the crux of the many IDSs that have proved efficient. Swarm intelligence [10] has also been used in order to try and decrease the training time of the IDS. A considerable number of hybrid schemes [11] are also employed, which proved more effective than the conventional models. In addition, there has been an alternate field of study [12], which take the human immune system (HIS) as an inspiration and derives an IDS for IoT networks. IDSs engineered [13,14] from HIS are commonly based on three different immune theories namely danger theory, negative selection, and clonal selection.

In this paper, a two-stage cross layer-based IDS is presented. Stage one is composed of five dedicated sniffers (DSs) which collect data from MAC and network layer. It is then fed to a random forest classifier, mounted on each DS, which generates a quantity known as correctly classified instances (CCIs). These CCIs are fed to a super node (SN) which is stage two. It performs a sliding window algorithm on all the CCIs collected from different DSs. This process calculates a parameter which we call the accumulated measure of fluctuation (AMoF). In addition, the SN performs an iterative linear regression process on the AMoF points. A detection threshold is chosen to separate the boundaries between the malicious and normal nodes. A key idea used in the proposed IDS, is that the variability of CCIs in the smaller size population, which represents the number of malicious nodes in the network is smaller than the variance of the larger size population, which represents the number of normal nodes in the network.

In this paper, we expand the previous work [8,15] and test the proposed architecture under a wide range of malicious activities such as blackhole and DDOS (flooding attack) and under other scenarios, such as mobility models. The proposed scheme is tested under two different mobility models; random way point (RWP) and Gauss Markov models (GM). The latter is used to add a more realistic mobility model which consists of a temporal correlation for nodes position based on certain parameters in this model.

This paper is divided into the following sections: Section 2 presents a brief survey of the related work. The system architecture of a multilevel detection approach utilizing random forest and linear regression is described in Section 3, while Section 4 presents a brief introduction about the blackhole attack and flooding attacks adopted in this paper. In Section 5, the experimental setup is explained in detail. Results and discussion are provided in Section 6. Finally, Section 7 concludes this paper.

2. Related Work

In this section, a simple survey for major machine learning techniques used in IDS for MANETS, WSN, and IoT is presented. The main material is taken from A. Amouri dissertation [16].

Deng et al. [17] proposed an IDS based on SVM classification algorithm for two types of IDS architecture, distributed and hierarchal. Detection rates well above 90% were achieved by using biasing in the feature selection.

An ensemble-based IDS for MANETs was proposed by Cabrera [18,19], where a three-level hierarchical system for data collection, processing, and transmission was described. The anomaly index at each level is calculated and the final decision is performed at the highest hierarchy. The authors used the receiver operating characteristic (ROC) curve and the corresponding area under curve (AUC) to characterize the performance of their proposed scheme. A C4.5 decision tree in conjunction with the CFA algorithm was used for detection purposes.

A dynamic learning method to detect blackhole attacks on AODV-based MANETs is proposed by Kurosawa et al. [20]. A dynamic training method in which the training data is updated at regular time intervals serves as the main concept for detecting malicious activity in the network. A simple

clustering algorithm is used to identify the malicious nodes. Detection rates versus node mobility are used for performance characterization, ranging from 70% to 84% for node mobility between 0 and 20 m/s.

In the proposed scheme by Bose et al. [21], a Bayesian classification algorithm, Markov chain construction algorithm and association rule mining algorithm for anomaly detection in MAC, routing and application layer, respectively for effective intrusion detection has been deployed. Detection rates of 94.33% and 0.8% false positive rate (FPR) were achieved at the global integration module.

An IDS based on neural networks and watermarking techniques was presented by Mitrokotsa and Komninos [22]. Detection rates around 90% with high false alarms (more than 20%) are reported. The detection rates were shown to be higher for longer periods of pause times.

Mitrokotsa et al. [23] analyzed the performance of well-known five supervised classification algorithms (the Naïve Bayes model, the linear model, the Gaussian mixture model, multilayer perceptron, and (SVM) model) used as a detection technique in detection engines for MANETs. Their results showed that the Naïve Bayes classifier has the poorest performance while the best performance is achieved with the multilayer perceptron classifier.

Azmoodeh and Choo [24], used the deep eigenspace learning for malware detection in “Internet Of (Battlefield) Things Devices”. The accuracy, precision, recall, and F-measure are: 99.68%, 98.59%, 98.37%, and 98.48%, respectively.

Doshi et al. [25] tested five machine learning algorithms to distinguish normal IoT packets from DoS attack packets. The algorithms are: (1) K-nearest neighbors “KDTree” algorithm; (2) support vector machine with linear kernel (LSVM); (3) decision tree using Gini impurity scores; (4) random forest using Gini impurity scores; (5) neural network. The random forest showed the best results among the tested classifiers for the precision, recall, F1, and accuracy tests.

Thamilarasu and Chawla [26] proposed a deep learning-based IDS for IoT, the following attacks were investigated: Blackhole attack, opportunistic attack, DDoS attack, Sinkhole attack, Wormhole attack, the TPR are 96.4%, 98%, 98.7%, 99%, 98%, respectively.

3. System Architecture

In this section, the system architecture for the cross-layered IDS is presented. The IDS is composed of two stages of detection as shown in Figure 1. At stage one, the dedicated sniffers (DSs) collect data, which is a packet count from both MAC and network layers as shown in Table 1. These are first-hand features collected through promiscuous mode which reduces the misleading data collected by direct reporting from the nodes themselves [27]. We use five DSs in this paper and they monitor an area of 1000 m².

Figure 1. A two stage cross layer IDS.

Every DS generates a CCI per reporting time (Tr). There are N instances of Tr as shown in Figure 1. Once two CCI samples are collected by the SN at stage two from each DS, an iterative process using linear regression which calculates the slope (β_1) and the threshold (δ) is performed as shown in Algorithm 1.

Linear regression explains the dependency between the dependent variable X and independent variable Y as [28],

$$Y_i = \beta_0 + \beta_1 X_i + \epsilon_i \quad (1)$$

where β_0 and β_1 are the model parameters. The errors ϵ_i are assumed to be independent $N(0, \sigma^2)$. The confidence interval for β_1 is given as

$$b_1 \pm \frac{t(n-2, 1-\frac{\alpha}{2})s}{\{\sum (x_i - \bar{x})^2\}^{1/2}} \quad (2)$$

where $t(n-2, 1-\frac{\alpha}{2})$ is the $100(1-\frac{\alpha}{2})$ percentage point of a t-distribution with $(n-2)$ degrees of freedom and the residual sum of squares s^2 . Equations (1) and (2), are used in Algorithm 1 to calculate the iterative fitted slope and the confidence interval based on the CCIs points collected from different DS regarding any node under test (NUT). A more detailed explanation about how the confidence interval is used in the detection characterization is presented in the Results Section 6.

It is important to mention that the values of the CCIs at the first stage does not yield information regarding the state of the tested nodes whether it is malicious or benign. It is the variability of the CCIs collected at the SN based on the sliding window-based algorithm as shown in Algorithm 1, that make the distinction between the state of two nodes feasible.

Algorithm 1 Calculating the AMoF, fitted slope, confidence intervals, and detection threshold

```

1: Input:  $CCI^{(DS_m)}_1, \dots, CCI^{(DS_m)}_N, \forall m \in n$ 
2: Output: AMoF, fitted slope ( $\beta$ ), detection threshold ( $\delta$ )
3: At the super node
4:  $\forall node \in NUT$  where the number of elements in NUT =  $l$ 
5: Receive  $CCI^{(S_n)}_1, \dots, CCI^{(S_n)}_N$  S.T  $CCI^{(NUT)}$  is  $N \times n$ 
6: Initialize  $Temp^{(S_i)}$ ,  $Norm\_Temp^{(S_i)}$ ,  $AMoF^{(S_i)}$ 
7: For  $i = 1$  to  $N$  do
8:   For  $j = 1$  to  $n$  do
9:      $TEMP_i^{(S_j)} \leftarrow |CCI_{i+1}^{(S_j)} - CCI_i^{(S_j)}| + TEMP_{i-1}^{(S_j)}$ 
10:     $Norm\_TEMP_i^{(S_j)} \leftarrow TEMP_i^{(S_j)} / 100$ 
11:   End for
12:    $AMoF_i^{(S_j)} \leftarrow Norm\_TEMP_i^{(S_j)} / n + AMoF_i^{(S_j)}$ 
13:   End for
14: Receive  $AMoF^{(NUT)}_1, \dots, AMoF^{(NUT)}_{N-1}$  S.T  $AMoF^{(NUT)}$  is  $l \times (N-1)$ 
15: For  $k = 1$  to  $N-1$  do
16:   For  $j = 1$  to  $l$  do
17:     If  $k \geq 2$  then
18:       Find  $\beta_k$  by solving (1)
19:       Find  $C_k$  by solving (2)
20:       Find time varying threshold  $\delta_k = \left( \frac{\max(C_k) - \min(C_k)}{2} \right) + \min(C_k)$ 
21:      $@k = 3$ 
22:      $\delta \leftarrow \delta_k$ 
23:     If  $\delta_k > \delta$ 
24:       Node is normal
25:     Else
26:       Node is malicious
27:     End for
28:   End for

```

4. Blackhole and DDoS Attack

In this section two types of malicious activities deployed in the experiments are described; blackhole attack and DDoS (flooding).

(a) Blackhole attack

The blackhole attack adopted in this work is based on [29], where a malicious node forges a fake route reply (RREP) that contains misleading information about its sequence number, the smaller the sequence number the fresher is the path, promoting him as the node having the shortest path to the destination node.

(b) DDoS (flooding)

It is a denial of service (DoS) based malicious activity which causes a disruption during the functioning of the network, by flooding the network with redundant data. In this paper, the route request (RREQ) flooding attack is used to simulate flooding activity [30]. DDoS is achieved by sending a large volume of traffic through the network which might lead to exhausting the network resources, overall bandwidth, and individual node resources.

5. Experimental Setup

Two extreme scenarios were tested based on node velocity and power level. Those scenarios are abbreviated as: NS1P3 and NS15P7 which refers to node velocity 1 m/s with power level of 3 dBm, and node velocity 15 m/s with power level of 7 dBm, respectively. The reason was to test the performance of the IDS under extreme connectivity levels. The connectivity is the lowest at NS1P3 and highest at NS15P7 [31].

The initial set of features used in the experiment are shown in Table 1. Those 12 features are collected from both MAC and network layer. A correlation-based attribute evaluator [32], is used to pick the most significant features based on their weight. The highest six frequent features that appeared in both NS1P3 and NS15P7 scenarios collected over the Tr , are shown in Figure 2. It is important to mention that those features are not optimum for the detection process, it presents some degree of redundancy which acts as noise. This is meant to test the IDS under suboptimal situations.

The data sets were generated by simulating a network with 30 nodes over an area of 1000 m² over 2000 s period. The network profile when no malicious activity is generated over 20 different seeds. The same procedure is applied when generating the malicious activity for blackhole attack and the flooding attack with designating three malicious nodes in each case. The flooding attack is based on RREQ. Two different mobility models are adopted in this paper, the RWP which is the benchmark for all mobility models and the GM which offers temporal correlation for the node's velocity. A memory value (α) is chosen equal to 0.5. It is a midpoint between a memoryless state where node's velocity at each time slot has no correlation (such as the RWP), and strong memory case where node's velocity at time slot is exactly as the pervious velocity [33].

The basic set of features used in the detection process are shown in Table 1 which will be reduced as mentioned before to six features for each type of attack. For the blackhole attack, the most frequent features obtained using the correlation-based attribute evaluator are: Route error transmitted (RERR_T), route error received (RERR_R), request-to-send transmitted (RTS_T), request-to-send received (RTS_R), PAYLOAD_T, RREP_R as shown in Figure 2a. The most frequent features in the case of flooding attack are: RTS_T, RTS_R, RREQ_T, RERR_R, RREQ_R, RERR_T as shown in Figure 2b.

The power levels, the node's mobility, and other simulation parameters are listed in Table 2. Notice that the total reporting points in the experiment are: Simulation time/ Tr = 2000/25 s = 80.

Table 1. Cross layer features.

Mac layer	Tx/Rx	Tx/Rx	Tx/Rx
	RTS	CTS	ACK
Network layer	Tx/Rx	Tx/Rx	Tx/Rx
	RREQ	RREP	RERR

Table 2. Simulation parameters.

No. of Nodes	30
Field area	1000 × 1000 m
Node speed	1 and 15 m/s
Simulation time	2000 s
Power levels	3 and 7 dBm
Routing protocol	AODV
Mobility model	RWP, GM
Reporting time (T_r)	25 s
Sampling time (T_s)	5 s

Figure 2. The most frequent features counted over all reporting times for the blackhole and flooding for both NS15P7 and NS1P3 scenarios: (a) Most frequent features in the blackhole case; (b) most frequent features in the flooding case.

6. Results and Discussion

In this section, the results are presented for extreme node velocities 1 and 15 m/s, and for the extreme power level 3 and 7 dBm. This represents in abbreviated form NS1P3 and NS15P7. Both scenarios are tested under blackhole (BH) and flooding (FL) attacks with both mobility models RWP, GM. Reporting time (T_r) is 25 s and sampling time (T_s) is 5 s. The detection parameters are true positive rate (TPR) also called recall, true negative rate (TNR), false positive rate (FPR), and false negative rate (FNR), precision, and F_1 score are shown in Equations (3)–(8). A detailed explanation for the detection performance using these equations and Algorithm 1, will be presented in the discussion section.

$$TPR = \frac{TP}{TP + FN} \quad (3)$$

$$TNR = \frac{TN}{TN + FP} \quad (4)$$

$$FPR = \frac{FP}{FP + TN} \quad (5)$$

$$FNR = \frac{FN}{FN + TP} \quad (6)$$

$$Precision = \frac{TP}{TP + FP} \quad (7)$$

$$F_1 = 2 * \frac{Precision.Recall}{Precision + Recall} \quad (8)$$

Based on [34], the TP, FN, FP, and TN are defined as:

True positive (TP): Represents the number of malicious nodes that have been correctly classified as malicious.

False negative (FN): Represents the number of malicious nodes that have been misclassified as benign nodes.

False positive (FP): Represents the number of benign nodes that have been misclassified as malicious.

True negative (TN): Represents the number of benign nodes that have been correctly classified as benign.

An example showing how the results were obtained based on Equations (3)–(8) and Algorithm 1 is shown below. Every fitted slope point has a lower bound (LB) and upper bound (UB), malicious nodes reside in the region below the threshold whereas the benign nodes reside in the region above the threshold. The errors arise from the fact that malicious nodes UBs pass the threshold towards the benign nodes region, and the benign nodes LBs pass the threshold towards the malicious nodes region.

(1) $TP = \text{sum}(UB(19) < \text{threshold}) + \text{sum}(LB(21) < \text{threshold})$;

It counts the points related to the malicious nodes (19 and 21) which their upper bound points are less than the threshold. Since the malicious nodes have smaller slopes than the benign nodes.

(2) $FP = \text{sum}(LB(13) < \text{threshold}) + \text{sum}(LB(23) < \text{threshold})$;

It counts the points related to the benign nodes (13 and 23) which their lower bound points are less than the threshold.

(3) $TN = \text{sum}(LB(13) > \text{threshold}) + \text{sum}(LB(23) > \text{threshold})$;

It counts the points related to the benign nodes (13 and 23) which their lower bound points exceed the threshold.

(4) $FN = \text{sum}(UB(19) > \text{threshold}) + \text{sum}(UB(21) > \text{threshold})$;

It counts the points related to the malicious nodes (19 and 21) which their upper bound points exceed the threshold.

The performance of the IDS which is characterized by the: TPR, FPR, TNR, FNR, and the F_1 score is presented in Tables 3–10.

It is noticed that the IDS can identify the malicious nodes with a near perfect detection of different scenarios with $TPR = 1$ always, which show robustness in identifying malicious nodes with different deployment scenarios (power levels and node mobility). The main difference in the performance of the IDS showed up when identifying benign nodes as malicious nodes with FPR varies from 1.28% to 4.49% in the NS15P7 scenario, Figures 3–6 and its corresponding tables, for RWP mobility and flooding attack in the first case and GM mobility and blackhole attack in the second case. This can be due to the nature of the blackhole attack, being more deceptive than the flooding attack since it does not just drop packets but tricks the designated traffic from source to destination to be forwarded through the malicious node. Moreover, the connectivity with RWP is better than GM which helps the data acquisition process that is needed to build the models for detection.

The second set of results are shown in Figures 7–10 and its corresponding tables. These results are related to the NS1P3 scenario. A deterioration in the FNRs is noticed, nearly three times as it results in NS15P7. FNR varies between 10–12%, it is related directly to the IDS capability of collecting enough packets at such low connectivity, leading to larger errors when compared to the NS15P7 scenario.

The F_1 score obtained for all the tested scenarios is above 90%. A highest F_1 score of 99.36% is obtained for the NS15P7 scenario under the DDoS attack with the RWP mobility. The lowest F_1 score of 93.94% is obtained for the NS1P3 scenario under the blackhole attack with GM mobility.

It is important to mention that choosing the location of the threshold, which is at the third iteration, has a significant effect on the results especially when dealing with the NS1P3 scenario. Notice the fluctuating nature of the fitted slopes figures, which makes choosing a proper location for the detection threshold, a hard task compared to the NS15P7 scenario.

Figure 3. The AMoF and the fitted slope for different nodes for scenario NS15P7: (a) The AMoF for different NUT; (b) the fitted slope for NS15P7_FL_RWP 25/5.

Table 3. Performance characterization for NS15P7_FL_RWP 25/5.

TPR	FPR	TNR	FNR	F_1
1	0.0128	0.9872	0	0.9936

Figure 4. The AMoF and the fitted slope for different nodes for scenario NS15P7: (a) The AMoF for different NUT; (b) the fitted slope for NS15P7_BH_RWP 25/5.

Table 4. Performance characterization for NS15P7_BH_RWP 25/5.

TPR	FPR	TNR	FNR	F ₁
1	0.0192	0.9808	0	0.9905

Figure 5. The AMoF and the fitted slope for different nodes for scenario NS15P7: (a) The AMoF for different NUT; (b) the fitted slope for NS15P7_FL_GM 25/5.**Table 5.** Performance characterization for NS15P7_FL_GM 25/5.

TPR	FPR	TNR	FNR	F ₁
1	0.0321	0.9679	0	0.9842

Figure 6. The AMoF and the fitted slope for different nodes for scenario NS15P7: (a) The AMoF for different NUT; (b) the fitted slope for NS15P7_BH_GM 25/5.**Table 6.** Performance characterization for NS15P7_BH_GM 25/5.

TPR	FPR	TNR	FNR	F ₁
1	0.0449	0.9551	0	0.9781

Figure 7. The AMoF and the fitted slope for different nodes for scenario NS1P3: (a) The AMoF for different NUT; (b) the fitted slope for NS1P3_FL_RWP 25/5.

Table 7. Performance characterization for NS1P3_FL_RWP 25/5.

TPR	FPR	TNR	FNR	F ₁
0.9936	0.1026	0.8974	0.0064	0.9483

Figure 8. The AMoF and the fitted slope for different nodes for scenario NS1P3: (a) The AMoF for different NUT; (b) the fitted slope for NS1P3_BH_RWP 25/5.

Table 8. Performance characterization for NS1P3_BH_RWP 25/5.

TPR	FPR	TNR	FNR	F ₁
1	0.1218	0.8782	0	0.9426

Figure 9. The AMoF and the fitted slope for different nodes for scenario NS1P3: (a) The AMoF for different NUT; (b) the fitted slope for NS1P3_FL_GM 25/5.

Table 9. Performance characterization for NS1P3_FL_GM 25/5.

TPR	FPR	TNR	FNR	F ₁
1	0.1090	0.8910	0	0.9483

Figure 10. The AMoF and the fitted slope for different nodes for scenario NS1P3: (a) The AMoF for different NUT; (b) the fitted slope for NS1P3_BH_GM 25/5.

Table 10. Performance characterization for NS1P3_BH_GM 25/5.

TPR	FPR	TNR	FNR	F ₁
0.9568	0.0833	0.9167	0.0432	0.9394

7. Conclusions

An extended study based on previous work for a multistage cross layer-based IDS is presented. A robust IDS is presented and tested under extreme deployment scenarios (power levels and node's

velocity). Detection rates (TPR) were near perfect in most of the scenarios presented. F_1 score varied between 93% and 99.36%. However, the limitation to this IDS is the false positive (FPR), which varied between 1.3% and 12% across various scenarios. The detection process is affected at the early stages of the fitted slope calculation. This is mainly due to the lack of packet counts that is related to the features used in the detection process. This problem mostly appears in the lower connectivity scenario, the NS1P3. A possible solution can be based on filtering these early stages of the fitted AMoF points.

Using a more complicated technique, based on the adaptive feature selection process at each reporting time, is another way to improve the performance and provide better differentiation between benign and malicious nodes during the early stages of the fitted slope process.

Author Contributions: A.A. is responsible for the idea formulation, investigation, formal analysis, deploying, and testing the system along with writing the original draft. V.T.A. helped with the software development, deployment, and editing the draft. S.D.M. was responsible for the general supervision, providing resources, and helped with the overall conceptualization. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to acknowledge Raju Manthena and Mohammad A. Bencherif for their inputs and their noteworthy contributions at every level of this project.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

In this appendix, a list of terms mentioned in this work are listed in Table A1.

Table A1. List of abbreviations mentioned in this paper.

Term	Meaning
NS1P3	Node velocity 1 m/s, power level 3 dBm
NS15P7	Node velocity 15 m/s, power level 7 dBm
GM	Gauss Markov mobility model
SN	Super node
DS	Dedicated sniffer
RWP	Random way point mobility model
BH	Blackhole attack
FL	Flooding attack
T_r	Reporting time
T_s	Sampling time
FS	Fitted slope
UB	Upper bound
LB	Lower bound
TPR	True positive rate
FPR	False positive rate
TNR	True negative rate
FNR	False negative rate
RTS	Request-to-send
CTS	Clear-to-send
ACK	Acknowledgement
RREQ	Route request
RREP	Route reply

Table A1. Cont.

Term	Meaning
RERR	Route error
NS15P7_FL_RWP 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type flooding, mobility model RWP, and reporting/sampling time of 25/5 s.
NS15P7_BH_RWP 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type blackhole, mobility model RWP, and reporting/sampling time of 25/5 s.
NS15P7_FL_GM 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type flooding, mobility model GM, and reporting/sampling time of 25/5 s.
NS15P7_BH_GM 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type blackhole, mobility model GM, and reporting/sampling time of 25/5 s.
NS1P3_FL_RWP 25/5	Scenario with corresponding node velocity of 1 m/s, power level of 3 dBm, attack type flooding, mobility model RWP, and reporting/sampling time of 25/5 s.
NS1P3_BH_RWP 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type blackhole, mobility model RWP, and reporting/sampling time of 25/5 s.
NS1P3_FL_GM 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type flooding, mobility model GM, and reporting/sampling time of 25/5 s.
NS1P3_BH_GM 25/5	Scenario with corresponding node velocity of 15 m/s, power level of 7 dBm, attack type blackhole, mobility model RWP, and reporting/sampling time of 25/5 s.

References

- Mishra, A.; Sudan, K.; Soliman, H. Detecting Border Intrusion Using Wireless Sensor Network and Artificial Neural Network. In Proceedings of the 6th IEEE international conference on distributed computing in sensor systems workshops (DCOSSW), Santa Barbara, CA, USA, 21–23 June 2010; pp. 1–6.
- Diro, A.A.; Chilamkurti, N. Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [[CrossRef](#)]
- Kaplanizis, S.; Shilton, A.; Nallasamy, M.; Sekercioglu, Y. Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Support Vector Machines. In Proceedings of the 3rd IEEE International Conference on Intelligent Sensors, Sensor Networks and Information, Melbourne, Australia, 3–6 December 2007; pp. 335–340.
- Amouri, A.; Jaimes, L.G.; Manthena, R.; Morgera, S.D.; Vergara-Laurens, I.J. A simple scheme for pseudo clustering algorithm for cross layer intrusion detection in MANET. In Proceedings of the 7th IEEE Latin-American Conference on Communications (LATINCOM), Arequipa, Peru, 4–6 November 2015; pp. 1–6.
- Sutharshan, R.; Leckie, C.; Palaniswami, M.; Bezdek, J.C. Anomaly Detection in Wireless Sensor Networks. *IEEE Wirel. Commun.* **2008**, *15*, 34–40.
- Amor, N.; Benferhat, S.; Elouedi, Z. Naive Bayes vs Decision Trees in Intrusion Detection Systems. In Proceedings of the 2004 ACM symposium on Applied computing, Nicosia, Cyprus, 14–17 March 2004; pp. 420–424.
- Lim, T.-S.; Loh, W.-Y.; Shih, Y.-S. A comparison of prediction accuracy, complexity, and training time of thirty-three old and new classification algorithms. *Mach. Learn.* **2000**, *40*, 203–228. [[CrossRef](#)]
- Amouri, A.; Morgera, S.; Bencherif, M.; Manthena, R. A Cross-Layer, Anomaly-Based IDS for WSN and MANET. *Sensors* **2018**, *18*, 651. [[CrossRef](#)] [[PubMed](#)]

9. Panhong, W.; Shi, L.; Wang, B.; Wu, Y.; Liu, Y. Survey on Hmm Based Anomaly Intrusion Detection Using System Calls. In Proceedings of the IEEE 5th International Conference on Computer Science & Education, Hefei, China, 24–27 August 2010; pp. 102–105.
10. Constantinou, K.; Kambourakis, G.; Maragoudakis, M. Swarm Intelligence in Intrusion Detection: A Survey. *Comput. Secur.* **2011**, *30*, 625–642.
11. Shahid, R.; Wallgren, L.; Voigt, T. Svelte: Real-Time Intrusion Detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674.
12. Alaparthi, V.T.; Amouri, A.; Morgera, S.D. A Study on the Adaptability of Immune Models for Wireless Sensor Network Security. *Procedia Comput. Sci.* **2018**, *145*, 13–19. [[CrossRef](#)]
13. Alaparthi, V.T.; Morgera, S.D. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory. *IEEE Access* **2018**, *6*, 47364–47373. [[CrossRef](#)]
14. Alaparthi, V.; Morgera, S.D. Modeling an Intrusion Detection System Based on Adaptive Immunology. *Int. J. Interdiscip. Telecommun. Netw.* **2019**, *11*, 42–55. [[CrossRef](#)]
15. Amouri, A.; Alaparthi, V.T.; Morgera, S.D. Cross Layer-Based Intrusion Detection Based on Network Behavior for IoT. In Proceedings of the 19th IEEE Wireless and Microwave Technology Conference (WAMICON), Sand Key, FL, USA, 9–10 April 2018; pp. 1–4.
16. Amouri, A. *Cross Layer-Based Intrusion Detection System Using Machine Learning for MANETs*; USF: Tampa, FL, USA, 23 April 2019.
17. Hongmei, D.; Zeng, Q.A.; Agrawal, D. SVM-Based Intrusion Detection System for Wireless Ad Hoc Networks. In Proceedings of the IEEE 58th Vehicular Technology Conference, Orlando, FL, USA, 6–9 October 2003; pp. 2147–2151.
18. Cabrera, J.; Gutiérrez, C.; Mehra, R. Infrastructures and Algorithms for Distributed Anomaly-Based Intrusion Detection in Mobile Ad-Hoc Networks. In Proceedings of the IEEE Military Communications Conference, Atlantic City, NJ, USA, 17–20 October 2005; pp. 1831–1837.
19. Cabrera, J.; Gutiérrez, C.; Mehra, R. Ensemble Methods for Anomaly Detection and Distributed Intrusion Detection in Mobile Ad-Hoc Networks. *Inf. Fusion* **2008**, *9*, 96–119. [[CrossRef](#)]
20. Kurosawa, S.; Nakayama, H.; Kato, N.; Jamalipour, A.; Yoshiaki, N. Detecting Blackhole Attack on Aodv-Based Mobile Ad Hoc Networks by Dynamic Learning Method. *Int. J. Netw. Secur.* **2007**, *5*, 338–346.
21. Bose, S.; Bharathimurugan, S.; Kannan, A. Multi-Layer Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks. In Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking, Chennai, India, 22–24 February 2007; pp. 360–365.
22. Mitrokotsa, A.; Komninos, N.; Douligeris, C. Intrusion Detection with Neural Networks and Watermarking Techniques for Manet. In Proceedings of the IEEE International Conference on Pervasive Services, Istanbul, Turkey, 15–20 July 2007; pp. 118–127.
23. Mitrokotsa, A.; Dimitrakakis, C. Intrusion Detection in Manet Using Classification Algorithms: The Effects of Cost and Model Selection. *Ad Hoc Netw.* **2013**, *11*, 226–237. [[CrossRef](#)]
24. Azmoodeh, A.; Dehghantanha, A.; Choo, K.K.R. Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning. *IEEE Trans. Sustain. Comput.* **2018**, *4*, 88–95. [[CrossRef](#)]
25. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35.
26. Thamilarasu, G.; Chawla, S. Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. *Sensors* **2019**, *19*, 1977. [[CrossRef](#)] [[PubMed](#)]
27. Sterne, D.; Balasubramanyam, P.; Carman, D.; Wilson, B.; Talpade, R.; Ko, C.; Balupari, R.; Tseng, C.-Y.; Bowen, T. A general cooperative intrusion detection architecture for MANETs. In Proceedings of the Third IEEE International Workshop on Information Assurance, College Park, MD, USA, 23–24 March 2005; pp. 57–70.
28. Draper, N.R.; Smith, H. Fitting a straight line by least squares. In *Applied Regression Analysis*, 3rd ed.; Wiley: Hoboken, NJ, USA, 1998; pp. 15–46.
29. Ehsan, H.; Khan, F.A. Malicious AODV: Implementation and Analysis of Routing Attacks in Manets. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 1181–1187.

30. Alokparna, B.; Vuppala, S.; Choudhury, P. A Simulation Analysis of Flooding Attack in Manet Using NS-3. In Proceedings of the IEEE 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, India, 28 February–3 March 2011; pp. 1–5.
31. Chu, T.; Nikolaidis, I. Node density and connectivity properties of the random waypoint model. *Comput. Commun.* **2004**, *27*, 914–922. [[CrossRef](#)]
32. Hall, M.A. *Correlation-Based Feature Selection for Machine Learning*; The University of Waikato: Hamilton, New Zealand, 1999.
33. Bai, F.; Helmy, A. A Survey of Mobility Models in Wireless Ad-Hoc Networks. *Wirel. Ad Hoc Sens. Netw.* **2006**, *206*, 1–30.
34. Detection Accuracy. Available online: <https://www.sciencedirect.com/topics/computer-science/detection-accuracy> (accessed on 15 September 2019).

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).