Sādhanā (2021)46:42
https://doi.org/10.1007/s12046-021-01573-9

Secure communication using θ-non-dominated sorting genetic algorithm

JASLEEN KAUR* and SUPREET KAUR

Department of Computer Science and Engineering, Punjabi University, Patiala, India
e-mail: jasleen.kr@yahoo.com

MS received 14 May 2020; revised 7 January 2021; accepted 11 January 2021

Abstract. With the growth in ad hoc devices, mobile ad hoc networks (MANETs) are extensively employed to realize different kinds of real-time applications. However, ad hoc devices suffer from numerous kinds of security attacks such as blackhole, grayhole, wormhole, etc. Therefore, an efficient trust management protocol is preferable. In this paper, a novel gradient boost classifier is proposed. Additionally, the hyper-parameters of gradient boost classifier are tuned using θ-non-dominated sorting genetic algorithm-III (θNSGA-III). Optimized link state routing (OLSR) protocol is employed for experimental analysis. A multi-class dataset is collected by implementing the blackhole, grayhole, and wormhole attacks on the OLSR. Comparative analysis reveals that the proposed θNSGA-III-based gradient boost classifier outperforms the competitive attack classification models.

Keywords. Trust evaluation; MANET; attacks; routing.

1. Introduction

The mobile ad hoc networks (MANETs) have shown their applicability in various kinds of applications such as surveillance systems. As MANETs do not have a stationary infrastructure, the mechanism varies for each MANET [1]. In MANETs, ad hoc nodes can move randomly and interchange data packets with each other wirelessly using a dynamic topology. Frequent topological alterations happen in MANETs because of this dynamic nature. They are widely accepted for unmanned networks and systems where telecommunication is absent [2]. Thus, the data communication in MANETs is achieved using direct links. Therefore, it is prone to various security threats. The attacks are often diverse, and a lack of preventive measures may cause serious losses [3]. A malicious node may provide false information to attack the network. It may drop or crack the potential information. In MANETs, the loss of data may occur while routing due to its lack of security. Hence many researchers have presented their research for providing secure routing in MANETs [4]. Thus, development of secure MANETs is an open area of research.

The recent trust-based approaches can improve the security of MANETs [5, 6]. To evaluate the trust, various performance measures of ad hoc nodes can be used. However, an inability to quantitatively represent these performance measures leads to inefficiency in the computation of trust values. Numerous algorithms have been implemented to evaluate trust values for an ad hoc node like fuzzy logic, trust administration, hybrid, etc. [7, 8]. The blackhole attack is a major attack that drastically reduces the throughput of MANETs [9, 10]. The attacker's node acts as the optimal route to the target node itself. If the attacker node receives the data packet from the source node, all obtained data packets are excluded from a routing network [11, 12]. Without notice participation and departure of nodes results in lack of trust relationship between nodes. In such circumstances, there is no guarantee that path between two nodes would be secure or free of malicious nodes. The presence of a single malicious node could lead to a repeatedly compromised node [13–15].

However, the design of efficient attack classification approach is still an open area of research. Therefore, in this paper, attack detection technique is redefined as a multi-class classification problem.

The main contributions are as follows:

1. An efficient trust management protocol is proposed.
2. Gradient boost classifier is designed to classify the ad hoc nodes as blackhole, grayhole, wormhole attacks or genuine node.
3. The hyper-parameters of gradient boost classifier are tuned using θ-non-dominated sorting genetic algorithm-III (θNSGA-III).
4. Optimized link state routing (OLSR) protocol is employed for experimental analysis.
5. A multi-class dataset is collected by implementing the blackhole, grayhole, and wormhole attacks on the OLSR.

*For correspondence
Published online: 20 February 2021

6. Comparative analysis reveals that the proposed θNSGA-III-based gradient boost classifier outperforms the competitive attack classification models.

The remaining paper is presented as follows. Related work about trust values for MANETs is presented in Section 2. The proposed trust mechanism model is mathematically presented in Section 3. Comparative analyses are discussed in Section 4. Section 5 concludes the paper.

2. Related work

Initially, a routing table was evaluated containing trust values. This table is then transmitted to all ad hoc nodes for secure communication. Trusted nodes were utilized for miners. However, to achieve an energy-efficient approach, one such node acts as a miner at a time [16]. The computed trust value and route cost were combined to achieve trust propagation. Trust entropy was then utilized to achieve secure communication among ad hoc nodes [17]. Routes with the minimum trust entropy are selected to add to the routing table [5]. The integrated space–terrestrial model was designed to improve the intercommunication coverage [18]. It has remarkably better secure communication performance.

The secure communication of data packets by utilizing on-demand trust-based model was proposed. It elects a minimum cost path along with good trust values to achieve secure communication [19]. A trust-based model for OLSR was proposed. However, it has not shown good performance against control packets [20]. A trust-vector and communication-pattern-based model was proposed that utilized every ad hoc node about the neighbors [21]. Improved trust anonymous on-demand communication model was proposed. It has restricted the unauthorized access of the data in the MANETs [22].

Fuzzy trusted dynamic source routing was proposed. It has utilized fuzzy values to compute the respective trust value of ad hoc nodes [23]. Recommendation-based trust approach was proposed utilizing clustering concept. Clusters based on trust values were formed for secure communication [24]. An improved OLSR protocol was proposed to achieve good performance against various security attacks [25]. A vector auto-regression-based trust approach was utilized to recognize attackers in the network. Ad hoc on-demand distance vector (AODV) and OLSR protocol were tested using the vector auto-regression-based trust approach [26]. Multiple loop-free routes were discovered to provide the secure transmission of data packets. Trust values along with the hop counts were utilized to realize the secure communication among ad hoc nodes [27]. The trust-based outlier recognization approach was designed for MANETs. It has shown significant improvement over stat-of-the-art trust models [28].

The problem of selfish ad hoc nodes were resolved in [29]. Ant colony optimization was utilized to achieve the secure communication among ad hoc nodes in dynamic MANETs [30]. Genetic algorithm (GA) was utilized to overcome the clustering load balancing problem in secure MANETs [31]. The dynamic shortest path communication was implemented utilizing GA-based immigrants and memory approaches [32].

A fault-tolerant ant look-ahead routing approach was propped to predict the secure communication link [33]. The reduction in the number of cluster heads was achieved utilizing the weighted clustering approach in [34]. Particle swarm optimization (PSO) was utilized to enhance the number of clusters for MANETs in [35]. GA was utilized to overcome the trust management issues of MANETs. The attributes like energy and distance were utilized to obtain the optimal cluster heads in [36].

3. Proposed trust evaluation model

3.1 *Gradient boost classifier*

Algorithm 1 Gradient boosting classifier

$\boldsymbol{u} \leftarrow \mathbf{0}$
for all T **do**
  for all l **do**
    $m_l \leftarrow \frac{\partial \ell}{\partial \hat{u}_l}$
    $n_l \leftarrow \frac{\partial^2 \ell}{\partial \hat{u}_l^2}$
  end for
  Train F according to Newton's step $\frac{-\boldsymbol{m}}{\boldsymbol{n}}$ using estimation of diagonals
  $\boldsymbol{u} \leftarrow \boldsymbol{u} + \nu F(\boldsymbol{C})$
end for
return obtained classification trees

The gradient boosting classifier [37] implements an ensembling model on various decision trees. XGBoost [38, 39] utilizes Newton's approach to enhance the 2^{nd}-order gradient loss by fitting the classification tree (see Algorithm 1). Here, T defines iterations and l shows instance of dataset; m_l and n_l represent the 1^{st} and 2^{nd} gradient, respectively. However, non-diagonal attributes in Hessian matrix were discarded during the Newton's step. It can degrade the performance of the gradient boosting classifier. Algorithm 2 shows the improved 2^{nd} order gradient model. The proposed model utilizes [40] to overcome the problems with Newton's approach, by improving the Newton's step as

Table 1. Nomenclature used in θNSGA-III.

Symbol	Definition
$\boldsymbol{\tau}$	Permutation vector
κ	Binary decision vector
$\mathcal{K}$	Random group of solutions
$\mathcal{R}$	Group of $\boldsymbol{\tau}'$, κ''
α	Random variable $\in$ [0 , 1]
ζ	Convert random solutions to hyper-parameters of gradient boosting
E_t	Elite population
$\boldsymbol{\tau}$	Optimal decision trees
κ	Optimal gradient boosting

$$\arg\min_{F} \sum_{l=1}^{s} \left(\ell(\tilde{u}_l) + \langle \ell'(\tilde{u}), F(\boldsymbol{v}_l) - \tilde{u}_l \rangle + \frac{1}{\eta} d(F(\boldsymbol{v}_l), \tilde{u}_l) \right) \tag{1}$$

Here, $\tilde{u}_l$ shows the rough approximation of u_l; $\ell'(\tilde{u})$ can be computed as follows:

$$\ell'(\tilde{u}) = \frac{1}{|T_k|} \sum_{\iota \in T_k} \ell'(\tilde{u}_\iota). \tag{2}$$

Here, T_k defines instance group of tree leaf (k) that considers instance l; $d(\cdot,\cdot)$ defines Bregman divergence according to the loss $\ell(\cdot)$ as follows:

$$d(F(\boldsymbol{v}_l), \tilde{u}_l) = \ell(F(\boldsymbol{v}_l)) - \ell(\tilde{u}_l) - \langle \ell'(\tilde{u}_l), F(\boldsymbol{v}_l) - \tilde{u}_l \rangle. \tag{3}$$

Plug $d(F(\boldsymbol{v}_l), \tilde{u}_l)$ and $\ell'(\tilde{u})$ in Eq. (1), by removing constant variables as

$$\arg\min_{F} \left(\ell(F(\boldsymbol{v}_l)) - \ell'(\tilde{u}_l) F(\boldsymbol{v}_l) + \frac{\eta F(\boldsymbol{v}_l)}{|T_k|} \sum_{\iota \in T_k} \ell'(\tilde{u}_\iota) \right). \tag{4}$$

Balancing process is implemented to minimize bias; the obtained loss can be defined as

$$N(F(\boldsymbol{C})) = \frac{a_l}{b_l} \left(\ell(F(\boldsymbol{v}_l)) - \ell'(\tilde{u}_l) F(\boldsymbol{v}_l) + \frac{\eta F(\boldsymbol{v}_l)}{|T_k|} \sum_{\iota \in T_k} \ell'(\tilde{u}_\iota) \right). \tag{5}$$

Finally, 1^{st} and 2^{nd} gradient of Newton's step can be computed, respectively, as

$$\tilde{m}_l = \frac{a_l}{b_l} \left(m_l - \ell'(\tilde{u}_l) + \frac{\eta}{|T_k|} \sum_{\iota \in T_k} \ell'(\tilde{u}_\iota) \right) \tag{6}$$

and

$$\tilde{n}_l = \frac{a_l}{b_l} n_l. \tag{7}$$

The probability of sample approximately corresponding to 2^{nd} gradient is $b_l = \min(1, \rho n_l)$.

Algorithm 2 Probability of sample approximately corresponding to Second order gradient

```
u ← 0
for all T do
  for all l ∈ {s} do
    m_l ← ∂ℓ/∂û_l
    n_l ← ∂²ℓ/∂û_l²
    b_l ← min(1, ρn_l)
    Obtain a_l ∈ {0,1} values by using Bernoulli attribute b_l
    m_l ← (a_l/b_l)(m_l − ℓ'(ũ_l) + ηℓ'(ũ))
    n_l ← (a_l/b_l) n_l
  end for
  Train F to Newton's step F(v_l) = −m_l/n_l by using the subgroup R = {l|a_l = 1}
  u ← u + νF(C)
end for
return obtained decision trees
```

3.2 *θ-non-dominated sorting genetic algorithm*

θ-non-dominated sorting algorithm– III (θ-NSGA-III) [41] is a well-known meta-heuristic technique. It can be used to solve many NP-hard problems. It has shown good convergence as compared with NSGA-III [42–44]. It utilizes dominance relation to enhance the results.

Algorithm 3 Obtain initial population

```
τ' ← Optimal decision trees.
τ'' ← { π_1, π_s, π_{s−1}, ..., π_2 }
κ' ← Apply gradient boosting on optimal decision trees.
κ'' ← ∅ R ← { ζ(τ', κ''), ζ(τ'', κ'')}
while z' = ∅ do
  l ← Consider decision tree l ∈ z' with maximum b_l/ω_l performance
  κ'' ← κ'' ∪ { l }
  κ' ← κ' \ { l }
  if (τ', κ'') is not dominated by (τ'', κ'') then
    R ← R ∪ { ζ(τ', κ'')}
  else
    R ← R ∪ { ζ(τ'', κ'')}
  end if
end while
K ← elect a random group of α × M solutions from R utilizing a normal distribution
L ← obtain a group of (1 − α) × M random solutions
E^(0) ← K ∪ L
return E^(0)
```

Table 1 shows the nomenclature used in this paper. Algorithm 3 shows the initial population generation for θNSGA-III-based gradient boosting tree. Initially, random population will be obtained using the normal distribution. Thereafter, the obtained solutions are encoded to the range of hyper-parameters of gradient boosting.

Algorithm 4 shows the proposed θNSGA-III-based gradient boosting tree classifier. Using the initial population, various decision trees are obtained. The obtained optimal decision trees are then ensembled to obtain the results of gradient boosting tree. Fitness of each random-population-based gradient boost tree is then evaluated. Thereafter, dominated and non-dominated solutions sets are obtained. Mutation and crossover operators are then utilized to obtain the sub solutions. Dominance relation (θ) is then utilized to sort the non-dominated solutions. Finally, if termination criteria gets satisfied then the final θNSGA-III-based hyper-parameters are returned for gradient boosting tree. The proposed model is then applied on the obtained trust evaluation dataset of MANETs.

Algorithm 4 Gradient boosting based on θ-non-dominated sorting genetic algorithm.

$\widehat{E_t} \leftarrow$ elect randomly $0.1M_t$ solutions from given elite E_t
for all $b \in \widehat{E_t}$ **do**
  $(\pi, z) \leftarrow$ decode b as hyper-parameters of gradient boosting
  for $l \leftarrow 1$ **to** NR_π **do**
    $\pi' \leftarrow$ obtain a random decision tree in π
    if (π', z) is not dominated by (π, z) **then**
      $(\pi, z) \leftarrow (\pi', z)$
    end if
  end for
  if (π, z) is not dominated by any combination in E_t **then**
    $E_t \leftarrow E_t \cup \{\zeta(\pi, z)\}$
  end if
  for $i \leftarrow 1$ **to** NR_z **do**
    $item \leftarrow$ elect randomly an $item \in \{1, 2, \ldots, h\}$
    if $item \in z$ **then**
      $z' \leftarrow z \setminus \{item\}$
    else
      $z' \leftarrow z \cup \{item\}$
    end if
    if (π, z') is not dominated by any solution in E_t **then**
      $E_t \leftarrow E_t \cup \{\zeta(\pi, z')\}$
    end if
  end for
end for
if $|E_t| > M_t$ **then**
  $E_t \leftarrow$ select M_t solutions obtain from θNSGA-III
end if

$\zeta(\boldsymbol{\tau}, \kappa)$ decomposes random individual $(\boldsymbol{\tau}, \kappa)$ to a hyper-parameters of gradient boosting tree.

Table 2. Simulation parameters.

Attribute	Value
MANET area	1000 m × 1000 m
Bandwidth	1 Mbps
Data rate	250 kbps
Number of ad hoc nodes	100–500
Moving speed	6 m/s
Transmission radius	200 m
Simulation time	200 s
Number of malicious nodes	1–10
Total number of data flows	3

Table 3. Malicious nodes combination.

No. of attackers	Blackhole	Grayhole	Wormhole
1	1	0	0
2	1	1	0
3	1	1	1
4	2	1	1
5	2	2	1
6	2	2	2
7	3	2	2
8	3	3	2
9	3	3	3
10	4	3	3

4. Performance analysis

4.1 *Dataset*

To obtain the dataset, initially, OLSR protocol is simulated on MATLAB software. Thereafter, three attacks – blackhole, grayhole, and wormhole – are applied on the obtained designed simulation environment. Multi-class dataset is then collected by labeling the attack cases as blackhole, grayhole, and wormhole attacks. If no attack is implemented then it is labeled as genuine node. The simulation parameters are demonstrated in Table 2. Ad hoc nodes are randomly placed in 1000 m × 1000 m area. The nodes are ad hoc in nature; therefore they have a speed of 6 m/s. Three different data traffic flows are also utilized at 250 kbps.

Table 3 demonstrates the combination of the attacker nodes utilized for building the dataset.

4.2 *Comparative analysis*

Figure 1 shows the routing overhead (in milliseconds) of θNSGA-III-based gradient boost classifier. It is observed

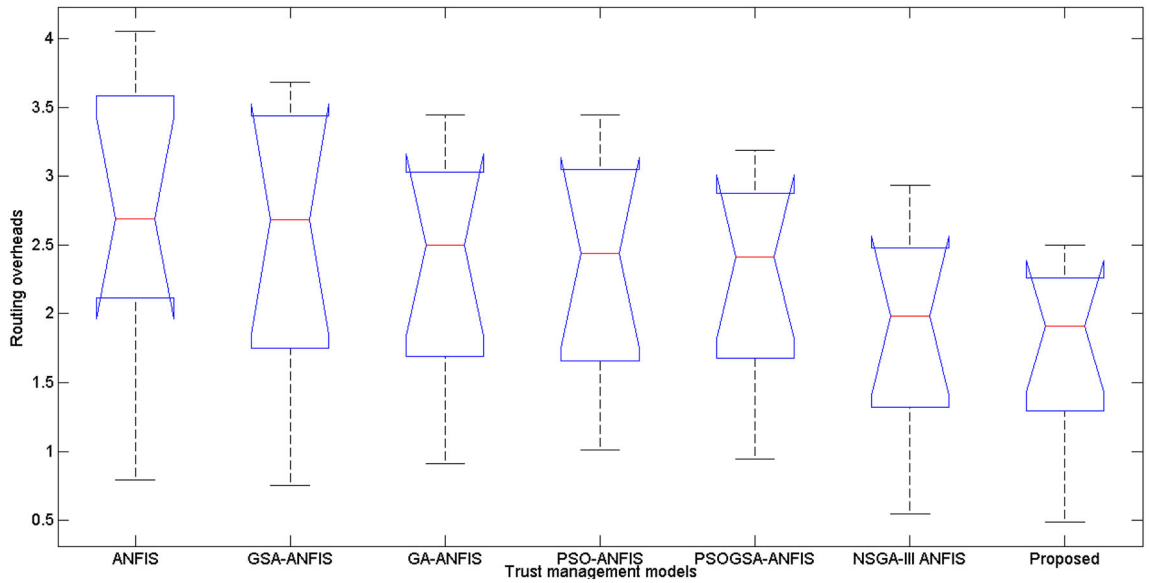

Figure 1. Analysis of routing overhead (in milliseconds) of θNSGA-III-based gradient boost classifier.

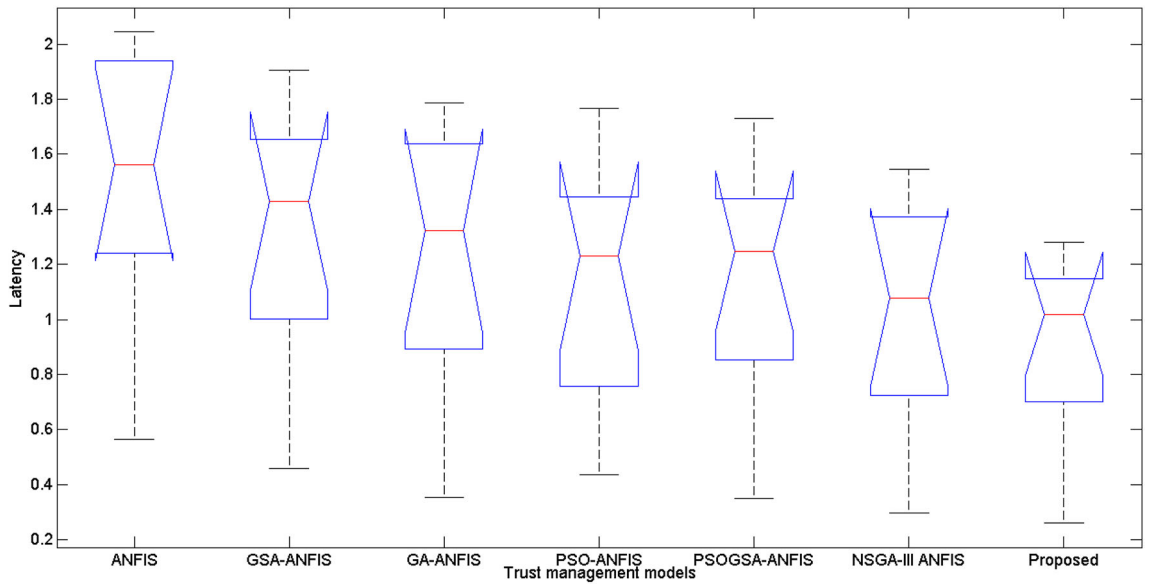

Figure 2. Latency analysis of θNSGA-III-based gradient boost classifier.

that θNSGA-III-based gradient boost classifier performs remarkably better than the existing models. θNSGA-III-based gradient boost classifier shows an average reduction in routing overheads of 1.2843%.

Figure 2 demonstrates the latency (in milliseconds) analysis of θNSGA-III-based gradient boost classifier. It is evaluated that θNSGA-III-based gradient boost classifier achieves remarkably better results than the existing models. θNSGA-III-based gradient boost classifier achieves an average reduction in latency of 1.3283%.

Figure 3 shows the packet delivery ratio analysis of θNSGA-III-based gradient boost classifier. It is observed

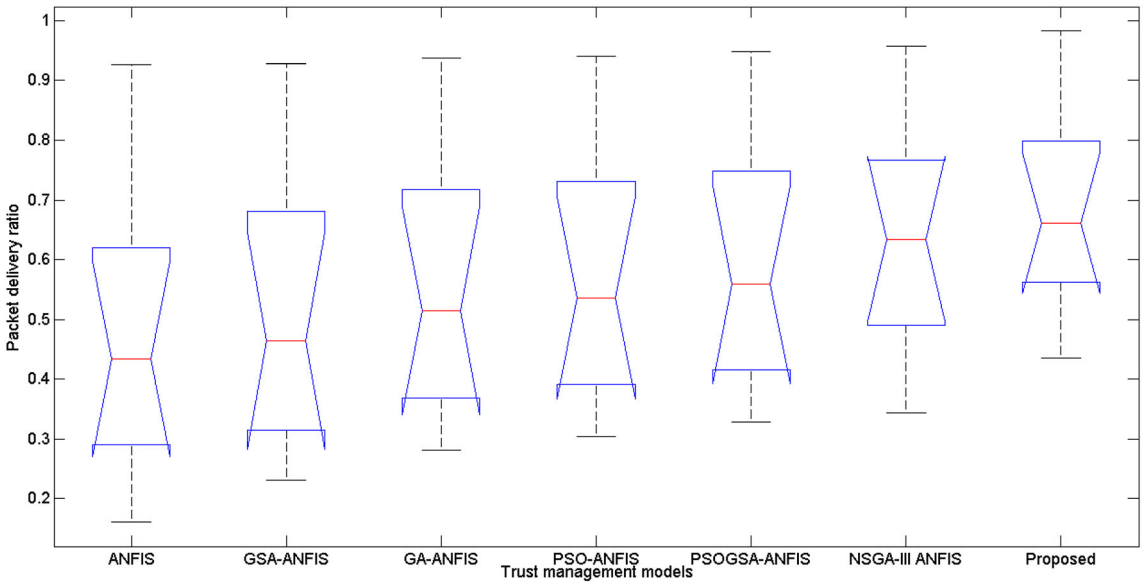

Figure 3. Packet delivery ratio analysis of θNSGA-III-based gradient boost classifier.

Trust evaluation

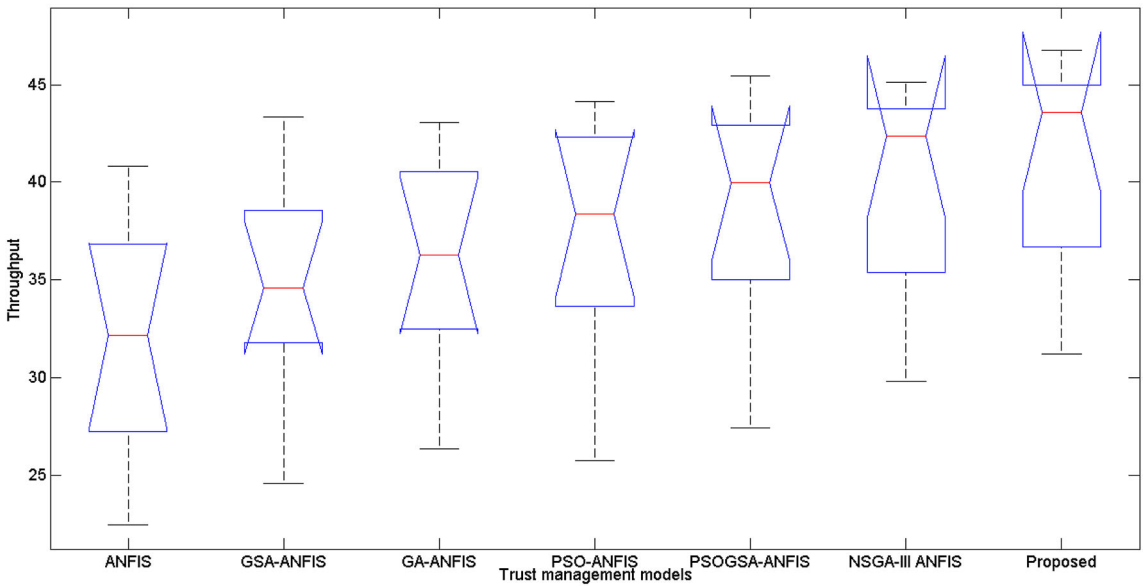

Figure 4. Throughput analysis of θNSGA-III-based gradient boost classifier.

that θNSGA-III-based gradient boost classifier achieves remarkably better packet delivery ratio values than the existing models. θNSGA-III-based gradient boost classifier achieves an average enactment in packet delivery ratio of 1.1472%.

Throughput analysis of θNSGA-III-based gradient boost classifier is depicted in Figure 4. It is observed that θNSGA-III-based gradient boost classifier achieves better average throughput values than the existing models. θNSGA-III-based gradient boost classifier achieves an average enactment in throughput of 1.2948%.

5. Conclusion

The attack classification problem of MANETs has been considered as a multi-class classification problem. A gradient boost classifier was proposed to classify a given node

as blackhole, grayhole, wormhole attack or genuine node. The initial parameters of gradient boost classifier were tuned using θNSGA-III. OLSR protocol was utilized for experimental analysis. The multi-class labeled dataset was collected by considering the blackhole, grayhole, and wormhole attacks on OLSR protocol. Extensive analysis reveals that θNSGA-III-based gradient boost classifier outperforms the competitive attack classification models in terms of throughput and PDR by 1.2948% and 1.1472%, respectively. The proposed trust evaluation model shows an average reduction in end to end latency and routing overheads by 1.3283% and 1.2843%, respectively..

References

[1] Bhawsar A, Pandey Y and Singh U 2020 Detection and prevention of wormhole attack using the trust-based routing system. In: *2020 Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC)*, July, pp. 809–814

[2] Rupasinghe L, Nawarathna C, Niroshan M A J, Kodithuwakku K A H, Kularathna M A S H and Liyanage S C G 2018 Trustworthy MANET routing ESTAODV implementation. In: *Proceedings of the 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)*, December, pp. 1–6

[3] Wang B, Ding L, Yang F, Qian L, Liu N 2019 Trust based partially distributed key management scheme for aeronautical ad hoc networks. In: *Proceedings of the 2019 25th Asia–Pacific Conference on Communications (APCC)*, November, pp. 449–454

[4] Karthick S, Sankar S P and Teen Y P A 2018 Trust–distrust protocol for secure routing in self-organizing networks. In: *Proceedings of the 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR)*, July, pp. 1–8

[5] Wang X, Zhang P, Du Y and Qi M 2020 Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network. *IEEE Access* 8: 47675–47693

[6] Subhankar Ghosh, Palaiahnakote Shivakumara, Prasun Roy, Umapada Pal and Tong Lu 2020 Graphology based handwritten character analysis for human behaviour identification. *CAAI Trans. Intell. Technol.* 5(1): 55–65

[7] Dhanya K, Jeyalakshmi C and Balakumar A 2019 A secure autonomic mobile ad-hoc network based trusted routing proposal. In: *Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI)*, January, pp. 1–6

[8] Hema Shekar Basavegowda and Guesh Dagnew 2020 Deep learning approach for microarray cancer data classification. *CAAI Trans. Intell. Technol.* 5(1): 22–33

[9] Travis Wiens 2019 Engine speed reduction for hydraulic machinery using predictive algorithms. *Int. J. Hydromechatron.* 2(1): 16–31

[10] Manjit Kaur, Dilbag Singh, Kehui Sun and Umashankar Rawat 2020 Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. *Future Gen. Comput. Syst.* 107: 333–350

[11] Naveena S, Senthilkumar C and Manikandan T 2020 Analysis and countermeasures of black-hole attack in MANET by employing trust-based routing. In: *Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, March, pp. 1222–1227

[12] Bhupendra Gupta, Mayank Tiwari and Subir Singh Lamba 2019 Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement. *CAAI Trans. Intell. Technol.* 4(2): 73–79

[13] Zalte S S and Ghorpade V R 2018 Intrusion detection system for MANET. In: *Proceedings of the 2018 3rd International Conference for Convergence in Technology (I2CT)*, April, pp. 1–4

[14] Sven Osterland and Jürgen Weber 2019 Analytical analysis of single-stage pressure relief valves. *Int. J. Hydromechatron.* 2(1): 32–53

[15] Renzong Wang, Hechun Yu, Guangzhou Wang, Guoqing Zhang, and Wenbo Wang 2019 Study on the dynamic and static characteristics of gas static thrust bearing with micro-hole restrictors. *Int. J. Hydromechatron.* 2(3): 189–202

[16] Biswas A K and Dasgupta M 2020 Modification of DSDV and secure routing using blockchain technology. In: *Proceedings of the 2020 4th International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech)*, October, pp. 1–5

[17] Kong R and Tong X 2020 Dynamic weighted heuristic trust path search algorithm. *IEEE Access* 8: 157382–157390

[18] Guo K, Wang D, Zhi H, Lu Y and Jiao Z 2020 A trusted resource-based routing algorithm with entropy estimation in integrated space–terrestrial network. *IEEE Access* 8: 122456–122468

[19] Hui Xia, Zhiping Jia, Xin Li, Lei Ju and Edwin H M Sha 2013 Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Netw.* 11(7): 2096–2114

[20] Shuaishuai Tan, Xiaoping Li and Qingkuan Dong 2015 Trust based routing mechanism for securing OSLR-based MANET. *Ad Hoc Netw.* 30: 84–98

[21] Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, Ming Gu and Kwok-Yan Lam 2010 Trust based routing for misbehavior detection in ad hoc networks. *J. Netw.* 5(5): 551

[22] Muthumanickam Gunasekaran and Kandhasamy Premalatha 2013 TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks. *IET Inf. Secur.* 7(3): 203–211

[23] Hui Xia, Zhiping Jia, Lei Ju and Youqin Zhu 2011 Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. *IET Wirel. Sens. Syst.* 1(4): 248–266

[24] Antesar M Shabut, Keshav P Dahal, Sanat Kumar Bista and Irfan U Awan 2014 Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Trans. Mobile Comput.* 14(10): 2101–2115

[25] Mohanapriya Marimuthu and Ilango Krishnamurthi 2013 Enhanced OLSR for defense against DOS attack in ad hoc networks. *Journal of Communications and Networks* 15(1): 31–37

[26] Revathi Venkataraman, Mullur Pushpalatha and T Rama Rao 2012 Regression-based trust model for mobile ad hoc networks. *IET Inf. Secur.* 6(3): 131–140

[27] Xin Li, Zhiping Jia, Peng Zhang, Ruihua Zhang and Haiyang Wang 2010 Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Inf. Secur.* 4(4): 212–232

[28] Nabil Djedjig, Djamel Tandjaoui, Faiza Medjek and Imed Romdhani 2020 Trust-aware and cooperative routing protocol for IOT security. *J. Inf. Secur. Appl.* 52: 102467

[29] Nilesh Marathe and Subhash K Shinde 2019 ITCA, an IDS and trust solution collaborated with ACK based approach to mitigate network layer attack on manet routing. *Wirel. Person. Commun.* 107(1): 393–416

[30] Hang Zhang, Xi Wang, Parisa Memarmoshrefi and Dieter Hogrefe 2017 A survey of ant colony optimization based routing protocols for mobile ad hoc networks. *IEEE Access* 5: 24139–24161

[31] Hui Cheng and Shengxiang Yang 2010 Genetic algorithms with immigrants schemes for dynamic multicast problems in mobile ad hoc networks. *Eng. Appl. Artif. Intell.* 23(5): 806–819

[32] Shengxiang Yang, Hui Cheng and Fang Wang 2009 Genetic algorithms with immigrants and memory schemes for dynamic shortest path routing problems in mobile ad hoc networks. *IEEE Tran. Syst. Man Cybern. Part C Appl. Rev.* 40(1): 52–63

[33] Surendran S and Prakash S 2015 An ACO look-ahead approach to QOS enabled fault-tolerant routing in MANETs. *China Commun.* 12(8): 93–110

[34] Bhaskar Nandi, Subhabrata Barman and Soumen Paul 2010 Genetic algorithm based optimization of clustering in ad hoc networks. *arXiv preprint* arXiv:1002.2194

[35] Hamid Ali, Waseem Shahzad and Farrukh Aslam Khan 2012 Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. *Appl. Soft Comput.* 12(7): 1913–1928

[36] Madasamy Kaliappan, Susan Augustine and Balasubramanian Paramasivan 2016 Enhancing energy efficiency and load balancing in mobile ad hoc network using dynamic genetic algorithms. *J. Netw. Comput. Appl.* 73: 35–43

[37] Lara Lusa *et al* 2017 Gradient boosting for high-dimensional prediction of rare events. *Comput. Stat. Data Anal.* 113: 19–37

[38] Adeola Azeez Ogunleye and Wang Qing-Guo 2019 Xgboost model for chronic kidney disease diagnosis. *IEEE/ACM Trans. Comput. Biol. Bioinform.* 17(6): 2131–2140

[39] Manjit Kaur, Dilbag Singh and Raminder Singh Uppal 2019 Parallel strength Pareto evolutionary algorithm-ii based image encryption. *IET Image Process.* 14(6): 1015–1026

[40] Daniel Chao Zhou, Zhongming Jin and Tong Zhang 2019 A fast sampling gradient tree boosting framework. *arXiv e-prints* arXiv:1911.08820

[41] Yuan Yuan, Hua Xu, Bo Wang and Xin Yao 2015 A new dominance relation-based evolutionary algorithm for many-objective optimization. *IEEE Trans. Evolut. Comput.* 20(1): 16–37

[42] Manjit Kaur, Dilbag Singh, Vijay Kumar and Kehui Sun 2020 Color image dehazing using gradient channel prior and guided l0 filter. *Inf. Sci.* 521: 326–342

[43] Anvita Gupta, Dilbag Singh and Manjit Kaur 2020 An efficient image encryption using non-dominated sorting genetic algorithm-iii based 4-D chaotic maps. *J. Ambient Intell. Hum. Comput.* 11(3): 1309–1324

[44] Manjit Kaur, Dilbag Singh and Vijay Kumar 2020 Color image encryption using minimax differential evolution-based 7D hyper-chaotic map. *Appl. Phys. B* 126(9): 1–19