Enhancement of MANET Security Using Modified Median Deviated Correlation and Regression Algorithms

Sayan Majumder[1†] and Debika Bhattacharyya[2††],

Gargi Memorial Institute of Technology, Institute of Engineering & Management, Kolkata, India

Abstract

MANET has drawn attention to researcher nowadays because of their uplifting demand. Wireless interface is endangered to different threats, as this network allows wireless technology and the procedure is very tough to defend or enhance the solidity of wireless network. In this analysis, least square and least deviated regression techniques are wielded to assess the design of wireless network safety. Accuracy percentage is also restrained for both algorithms. Then absolute deviation correlation over median is plied to inflate the security due to worm hole, black hole and Sybil attack. To build up the security, we have tried to polish up the throughput, delay variance, route discovery time and hops per second using our MAD Correlation (Absolute Deviation over Median) algorithm. AODV routing algorithm is employed here. We have implemented our algorithms in MATLAB and at last made a comparative analysis on how our algorithms enhanced the safety in MANET from these threats.

Keywords:

AODV, Correlation, LAD, MLS, MANET, Median, Regression

1. Introduction

Nodes of MANET serve as routers. Various data blocks are connected from starting node to destination, through different algorithms like DSR, AODV etc. among which we have chosen AODV algorithm, which uses conventional routing tables [1]. After training with 70%- 80% of data from data sets, we have to inspect the model with remaining data. Machine learning algorithms use trust vector to speculate the particular design from the model. Further we can divide machine learning technique into Classification [2] and Regression [3]. A dynamic, multi hop fashioned way is established by mobile ad hoc network [4] which is a variety of self- governing nodes. These nodes are at liberty to attach with network or detach from it any time because of their independency nature. Because of this, MANET [5] is not shielded to different threats.

Here, nodes are not trustworthy, because access points are not present between them. Due to diffuse design, many complex attacks are encountered by ad hoc network like, worm hole, black hole, Sybil etc.

Wormhole attack [6] creates a fake route between source node and terminating nodes. There is an intensity of prospect of replicating the data packets in between that route. It appears to be like that those affected routes take lesser amount of time to reach destination than the original one. We have enhanced the security of MANET by improving the delay variance, route discovery time, average throughput using our Median Absolute Deviation Correlation [7] Technique.

False presentation of data and without Advancing those, Black hole attack actually snatches the data packets. Path request and reply message must be communicated between two nodes. Affected node sends wrong information to the starting node in this event.

So, the packets full of data are dropped one after another by the affected node in black hole attack. Attackers can also grab in MANET by nodes that interact with one another without the central base station, and a spiteful node acts as different identities, called a Sybil attack [8]. Different conformity may be taken by Sybil [9] attackers, to impart messages to different path- ways.

To predict the pattern and mitigate wormhole attack [10] in MANET, many researchers have already used statistical experiments. Using SAM, we can achieve the multi path routing, for which worm hole attack is exposed. SAM has no concept of security and architecture. A dependable route is also researched by Cross Correlation process.

Absolute deviation about median is better approach to mitigate various attacks in ad hoc network. To do so, we have constructed an algorithm by using of which we have deduced the different quality of services of MANET and then tried to enhance them. Within this research, at first, we have estimated the pattern of different attacks using two modified regression techniques, based on deviated and squared value of two variables, packets sent to packets dropped. Following that, accuracy is also calculated for both of the algorithms and finally made a collation among them. After prediction, we have mitigated the Sybil, black hole and worm hole attacks using our modified algorithm. We have observed hop count, throughput, delay variance. If the utility of correlation of these factors scatters a lot

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.58

throughout a particular path, we can avoid those paths to strengthen the safety. In the context of low overhead, our algorithm is preferable approach than classical correlation analysis.

2. Background

In 2012, Fraser Cadger et. Al proposed machine learning methods centered on Regression [11], which predict the coordinates as continuous variable. Main target of this scrutiny was to find location prediction using different machine learning algorithms.

M. Thebiga and R. Sujipramila explained a secured and trustworthy method [12] to mitigate Black Hole attack in MANET, which is nothing but the advancement of correlation technique. They also proved the proposed method on different MANET quality of service. RRE and RREP techniques are also used by them in the algorithm and they used DSR routing technique.

Adwan Yasin and Mahmoud Abu Zant [13] enhanced AODV routing protocol using a novel tiimers-baiting technique. By using this technique, Black Hole attack was identified and isolated.

In the year 2014, Ankita Sharma and Sumit Vashistha modified the normal AODV protocol by minimizing the drop under MAC [14] error.

Lediona Nishani and Marenglen Biba completed a thorough survey on four different approaches of machine learning to detect intrusion [15] on MANET and published in 2016.

3. Proposed Methodology

To predict the degree of linearity or pattern of the different security attacks in ad hoc network, we have used two regression algorithms-

a. Least Square regression

b. Least Absolute Deviation regression

3.1. MLS Regression Algorithm for MANET

We have firstly sent some data packets from source to destination and calculated number of packets dropped. Then we have applied these two regression algorithms. After plotting the graph, we can observe that it follows a certain linear pattern. After that, best fitting curve is also measured. To predict the best fitting curve for (m1, n1), (m2, n2) ... (m*k,* n*k*), Where- m*i* = Number of Packets dropped. n*i* = Number of Packets sent.

Algorithm 1

Step 1: Find the median of the lost data packets (m) by security attacks and packets sent,

$X= \Sigma^k k\ m_i / k$

$Y= \Sigma^k n_i / k$

Step 2: Find the correlation coefficients between loss of packets and sent (slope of the line).

$t= \Sigma^k k\ (m_i - m^/)\ (n_i - n^/)/ n\ (x_i - x^/)^2$

Step 3: Find the data packets sent (y) intercept.

$b= n^/ - tm^/$

Step 4: Use the slope t and the y intercept b to predict the pattern.

$Y= n + b\ (m_i - m^/)$

Finish: Plot the graph accordingly.

3.2. LAD Regression Algorithm for MANET

To calculate the relation between two variables, $E= \Sigma e^2 = \Sigma k\ |(m_i - m^/)|$ is computed as least absolute deviation that is absolute value of deviated variable is taken in place of squared value.To predict the best fitting curve for (m_1, n_1), (m_2, n_2) . . . (m_k, n_k), Where-m_i = Number of Packets dropped. n_i = Number of Packets sent.

Algorithm 2

Step 1: Find the average of the lost data packets

(m) by security attacks and packets sent (n).

$X= \Sigma^k m_i / k$

$Y= \Sigma^k n_i /k$

Step 2: Find the correlation coefficients between loss of packets and sent (slope of the line).

$t=\Sigma^k k\ (m_i - m^/)\ (n_i - n^/)/n\ |(x_i - x^/)|$

Step 3: Find the data packets sent (y) intercept.

$b= n^/ - tm^/$

Step 4: Use the slope t and the y -intercept b to

predict the pattern.

$Y= n + b\ (m_i - m^/)$

Finish: Plot the graph accordingly.

After the prediction, we have to enhance the security features by modifying delay variance, throughput, hops count and average time taken by the three attacks viz. worm hole, black hole and attacks. For this, we have used modified correlation algorithm, which is MAD correlation algorithm (Median Absolute Deviation) [16].

Algorithm 3

AD Correlation [17] about Median of random variable y and z,

DCORR $_{(y, z)}$ = ¼[(D(y_1+z_1))2 - (D(y_1-z_1))2]

Where, y_1= [y- E(y)] / D(y), z_1= [z- E(z)] / D(z)

Median deviated correlation algorithm to enhance the security,

Step 1. Origination of node s, set s = 0 to s_{max}.

Step 2. Set s= s_k - T_k. (Number of transmission node)

Step 3. Generation of route path from T_k to destination.

Step 4. Start counter and then pass route message source.

Step 5. Receive reply message from route.

Step 6. If the interrelation is malicious, jump into step8.

Step 7. Else, go on with the packets forwarding process.

Step 8. Compute $corr_{coeff}$ from data.

Step 9. If the value of AD-$Corr_{coeff}$ is much more than normal value, jump

into step11.

Step 10. Otherwise, continue the packet accelerating.

Step 11. Report intruder.

4. Results and Discussions

Using Mat Lab simulator, we have first predicted the character of pattern between packets sent to dropped for 3 attacks. We have used both the regression techniques to do so. After that, using our MAD correlation [17] algorithm, we have enhanced the security by modifying throughput, delay variance, hop count, average time taken. Nine nodes are taken as input.

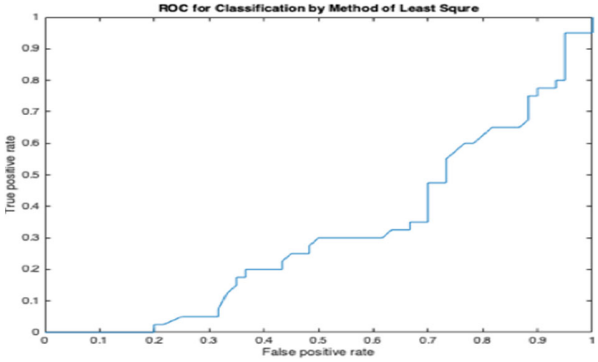

Fig. 1 Prediction of Worm Hole Attack Using the Method of Least Square Regression.

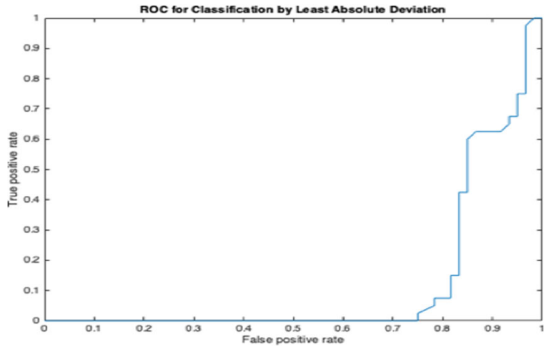

Fig. 2 Prediction of Worm Hole Attack Using the Least Absolute Deviation Regression.

From the figures 1 and 2, we can observe the projection of worm hole attack follows mostly linear pattern using the two algorithms. So, we can also conclude the best fitting curve or straight line to appraise the degree of relatedness between the packets sent to packets dropped by this attack. Similarly, the prediction for other two attacks are also recorded below, which also follow the linear pattern.

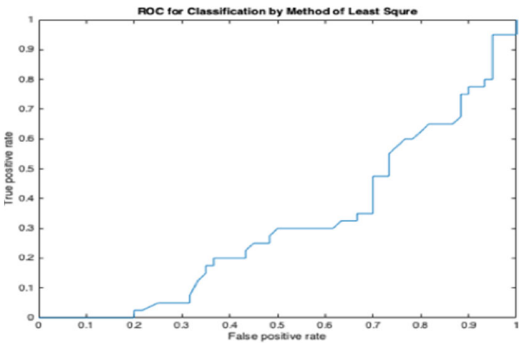

Fig. 3 Prediction of Black Hole Attack Using Method of Least Square Regression.

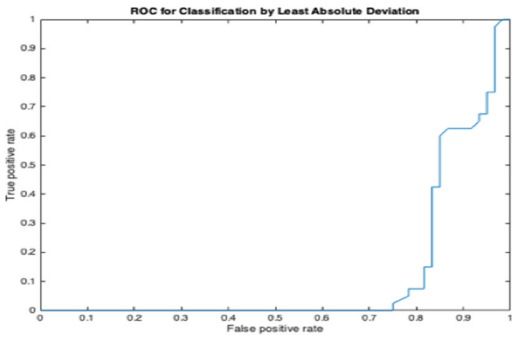

Fig. 4 Prediction of Black Hole Attack Using Least Absolute Deviation Regression.

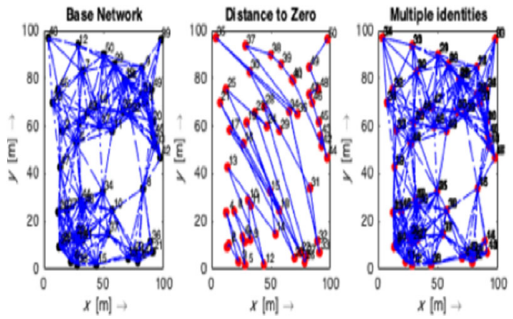

Fig. 5 Sybil Attack Scenario

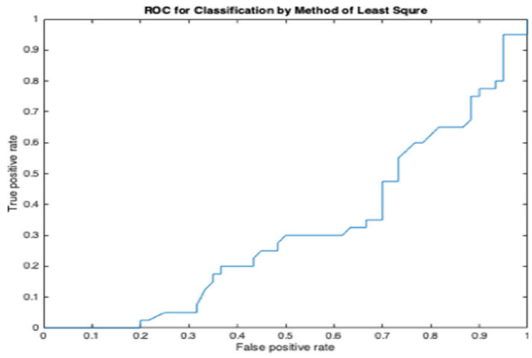

Fig. 6 Prediction of Sybil Attack Using the Method of Least Square Regression

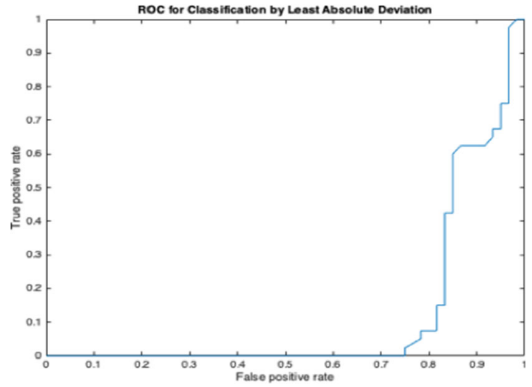

Fig. 7 Prediction of Sybil Attack Using the Least Absolute Deviation Regression

Some quality of services are enlisted for three attacks and tried to enhance them using our median absolute deviation correlation algorithm. If the MAD correlation coefficient is much greater than 0.95, then the path is signified as affected and we can avoid the path. By improving the factors, we can enhance the reliability of MANET [18].

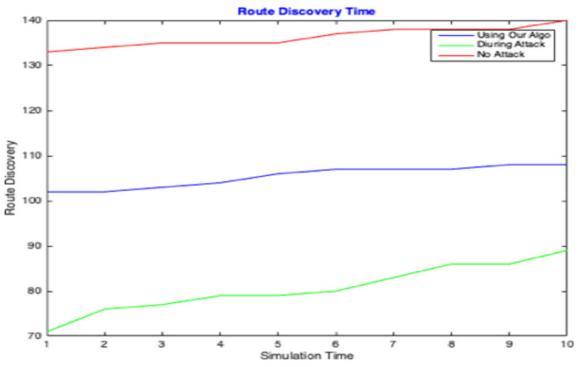

Fig. 8 Enhanced Average Route Discovery Time of Worm Hole Attack.

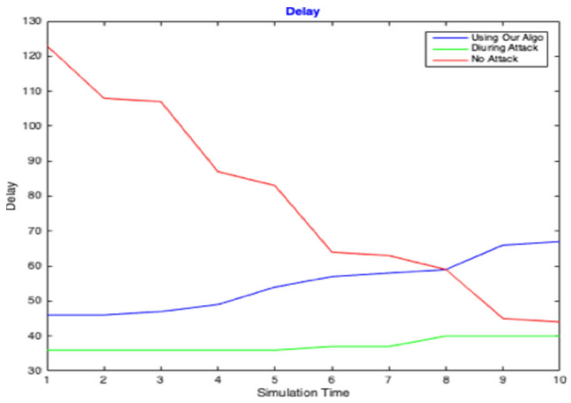

Fig. 9 Enhanced Delay Variance of Worm Hole Attack.

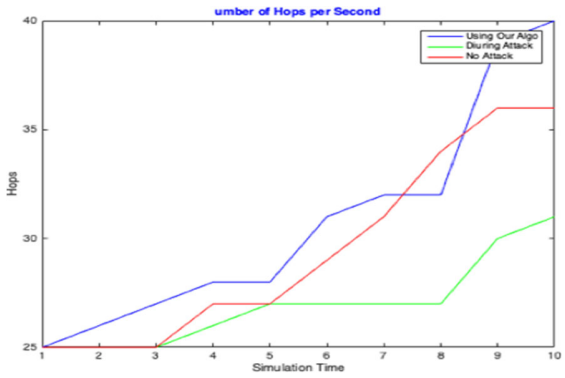

Fig. 10 Enhanced Hop Count of Worm Hole Attack.

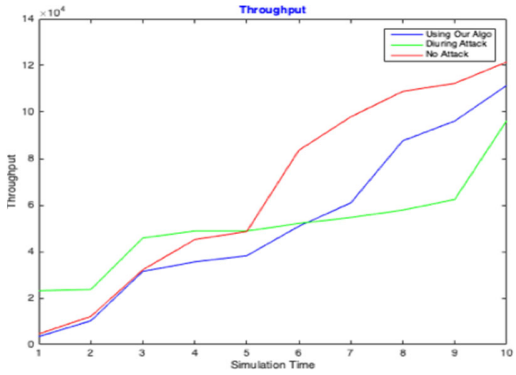

Fig. 11 Enhanced Throughput of Worm Hole Attack.

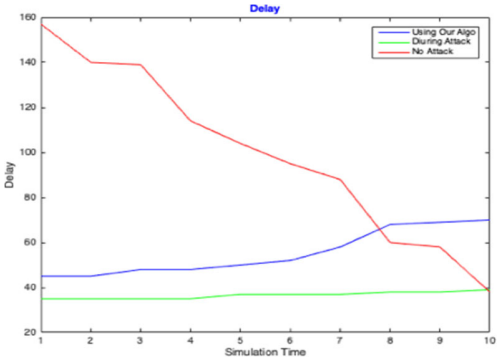

Fig. 12 Enhanced Delay Variance of Black Hole Attack.

The black hole attack is prevented using our algorithm and after that delay variance and other features are also modified by which security of ad hoc network got enhanced.

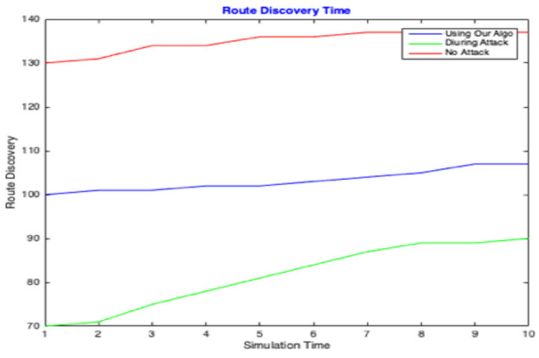

Fig. 13 Enhanced Average Route Discovery Time of Black Hole Attack.

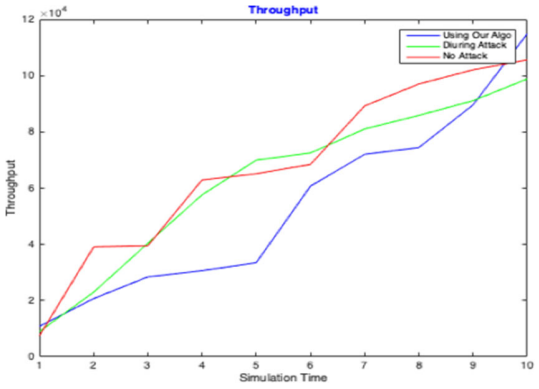

Fig. 14 Enhanced Throughput of Black Hole Attack.

The blue lines in the figure 14 and 15 are showing the features using modified algorithm [19] which is better than previous condition, that is when attack was committed.
For each figure, this is observed from our simulated result, that our algorithm works well for quality of services [20] of three security attacks in wireless ad hoc network very well.

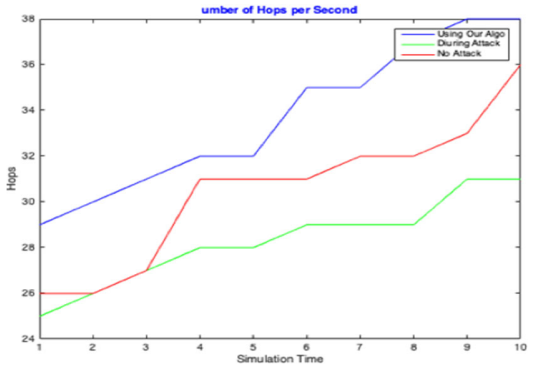

Fig. 15. Enhanced Hop Count of Black Hole Attack

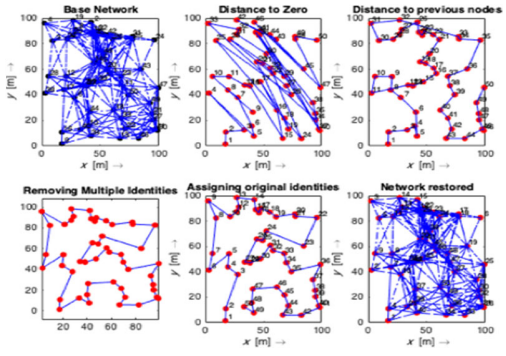

Fig. 16. Prevention of Sybil Attack

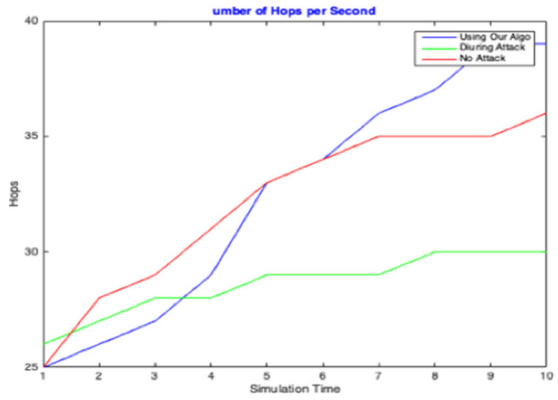

Fig. 17 Enhanced Hop Count of Sybil Attack.

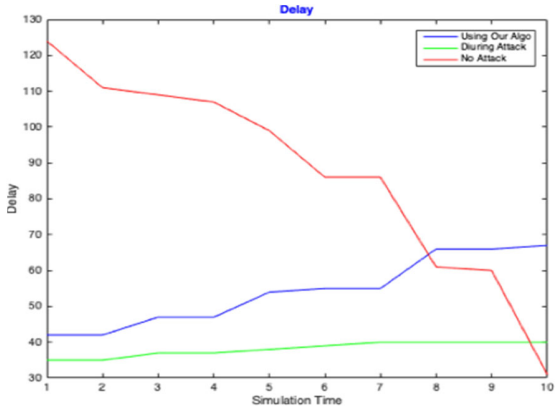

Fig. 18 Enhanced Delay Variance of Sybil Attack.

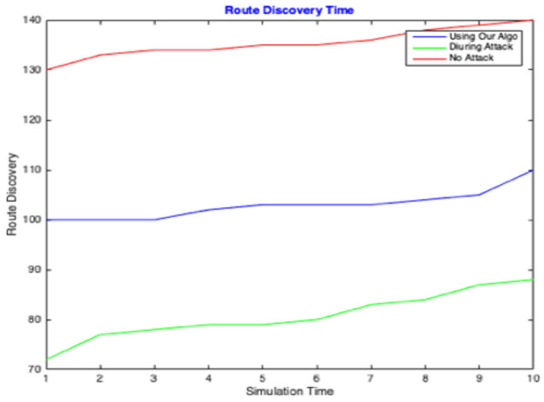

Fig. 19 Enhanced Average Route Discovery of Sybil Attack.

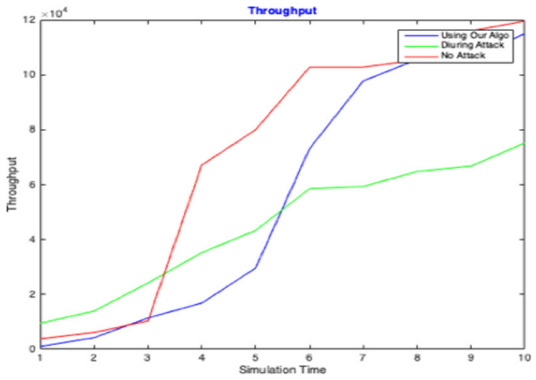

Fig. 20 Enhanced Throughput of Sybil Attack.

5 Conclusions

The pattern of packets dropped with the packets sent by three different attacks are estimated 1st, viz. worm hole, black hole and Sybil attacks

.

To do so, two regression techniques are applied as MLS and LAD. We have observed that this pattern is mostly linear for both of the algorithms but least square regression gives more accuracy than absolute deviation regression for all the three attacks. When outliers are present in our dataset, then least absolute deviation gives better result.

After that, we have mitigated the security attacks using our median deviated correlation algorithm. Whenever the correlation coefficient is very high for any route, we can avoid that path. By this technique we have enhanced the Quality of Service as Throughput, Delay Variance, Average route discovery time and number of Hops. From the graph, we can say that our Absolute Deviation algorithm has minimized the attack caused by worm hole, black hole and Sybil. So, we can say that our ad hoc network security is also got enhanced.

Here, we have presented a comparative study to establish the effectiveness of our algorithm on 3 different security attacks.

Table 1: Comparative Study of Effectiveness of Our Proposed Absolute Deviation Algorithm about Median Between MANET Security Attacks

Worm Hole Attack	***Black Hole Attack***	**Sybil Attack**
Predicted pattern is mostly linear	Predicted pattern is mostly linear	Predicted pattern is mostly linear
MAD $Corr_{coeff}$ value is 0.96 or higher	MAD $Corr_{coeff}$ value is 0.94 or higher	MAD $Corr_{coeff}$ value is 0.94 or higher
Security attacks are enhanced by mostly 82%	Security attacks are enhanced by mostly 78%	Security attacks are enhancedby mostly 75%

References

1. Qiu, J.; Wu, Q.; and Ding, G. *(2016).* A survey of machine learning for big data processing. *EURASIP J. Adv. Signal Process., (67)* https://doi.org/10.1186/s13634-016-0355-x
2. Kotsiansis, S.B.; Zaharakis, I.D.; and Pintelas, P.E. (2006). Machine Learning: a review of classification and combining techniques. *Artif Intell Rev* **26,** 159–190. https://doi.org/10.1007/s10462-007-9052-3
3. Taylor R.D. (2015). Multiple Regression Analysis as a Retail Site Selection Method: An Empirical Review. In: Bellur V. (eds) The 1980's: A Decade of Marketing Challenges. Developments in Marketing Science: Proceedings of the Academy of Marketing Science. Springer, Cham.
4. S., Majumder; and Bhattacharyya, D. (2018). Mitigating wormhole attack in MANET using absolute deviation statistical approach, *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2018, pp. 317-320. doi: 10.1109/CCWC.2018.8301780
5. Majumder, S.; and Bhattacharyya, D. (2020). Relation Estimation of Packets Dropped by Wormhole Attack to Packets Sent Using Regression Analysis. In: Mandal J., Bhattacharya D. (eds) Emerging Technology in Modelling and Graphics. Advances in Intelligent Systems and Computing, vol 937. Springer, Singapore. https://doi.org/10.1007/978-981-13-7403-6_49
6. Dutta, N.; and Singh, M.M. (2019). Wormhole Attack in Wireless Sensor Networks: A Critical Review. In: Mandal J., Bhattacharyya D., Auluck N. (eds) Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol 702. Springer, Singapore. https://doi.org/10.1007/978-981-13-0680-8_14
7. Jia, Riheng (2017). "Optimal Capacity–Delay Tradeoff in MANETs With Correlation of Node Mobility." *IEEE Transactions on Vehicular Technology* 66, 1772- 1785.
8. Jamshidi, M.; Zangeneh, E.; and Esnaashari, M. (2019). A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It.*Wireless Pers Commun* **105,** 145–173 https://doi.org/10.1007/s11277-018-6107-5
9. S., Abbas; M., Merabti; D., Llewellyn-Jones; and K., Kifayat (2013) ."Lightweight Sybil Attack Detection in MANETs," in IEEE Systems Journal, vol. 7, no. 2, pp. 236-248.
10. Sayan, Majumder; and Debika, Bhattacharyya, "Comparative Study between Modified DSR and AODV Routing Algorithms to Improve the PDF Due to Wormhole Attack in MANET", International Journal of Scientific Research and Review, volume-8, issue- 1, pp. 1095- 1110.
11. Cadger, F.; Curran, K.; Santos, J.; and Moffett, S. (2012). MANET Location Prediction Using Machine Learning Algorithms. In: Koucheryavy Y., Mamatas L., Matta I., Tsaoussidis V. (eds) Wired/Wireless Internet Communication. WWIC 2012. Lecture Notes in Computer Science, vol 7277. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30630-3_15
12. Thebiga, M.; and SujiPramila, R. (2020). A New Mathematical and Correlation Coefficient Based Approach to Recognize and to Obstruct the Black Hole Attacks in Manets Using DSR Routing. *Wireless Pers Commun* **114,** 975–993. https://doi.org/10.1007/s11277-020-07403-1
13. Yasin, A.; and Abu, Zant, M. (2018). Detecting and isolating black-hole attacks in MANET using timer based baited technique. *Wireless Communications and Mobile Computing*.
14. Sharma, A.; and Vashistha S. (2014). Improving the QOS in MANET by Enhancing the Routing Technique of AOMDV Protocol. In: Satapathy S., Avadhani P., Udgata S., Lakshminarayana S. (eds) ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I. Advances in Intelligent Systems and Computing, vol 248. Springer, Cham. https://doi.org/10.1007/978-3-319-03107-1_41
15. Nishani, L.; and Biba, M. (2016). Machine learning for intrusion detection in MANET: a state-of-the-art survey. *J Intell Inf Syst* **46,** 391–407. https://doi.org/10.1007/s10844-015-0387-y
16. Gong, X.; Shen, L.; and Lu, T. (2019). Refining Training Samples Using Median Absolute Deviation for Supervised Classification of Remote Sensing Images. *J Indian Soc Remote Sens* **47,** 647–659. https://doi.org/10.1007/s12524-018-0887-7
17. Amir, E.A.H.E. (2012). On uses of mean absolute deviation: decomposition, skewness and correlation coefficients. *METRON* **70,** 145–164. https://doi.org/10.1007/BF03321972
18. Arappali, N.; and Rajendran, G.B. (2020). MANET security routing protocols based on a machine learning technique (Raspberry PIs). *J Ambient Intell Human Comput*. https://doi.org/10.1007/s12652-020-02211-8
19. Xiuqing, Z.; and Jinde, W. (2005). LAD estimation for nonlinear regression models with randomly censored data. *Sci. China Ser. A-Math.* **48,** 880–897.

https://doi.org/10.1007/BF02879071

20. Vandna, Rani, Verma; D.P., Sharma; and C.S., Lamba (2019). "Improvement in QoS of MANET Routing by finding optimal route using Mobile Agent paradigm and Intelligent Routing Decision using Fuzzy Logic Approach", *Computing Power and Communication Technologies (GUCON) 2019 International Conference on*, pp. 725-730.

Sayan Majumder, received his B.Tech degree in Computer Science & Engineering from Swami Vivekananda Institute of Technology, Kolkata, India. He was awarded his M.Tech degree in Computer Science & Engineering from Netaji Subhas Engineering College, Kolkata, India. He is pursuing his Ph.D in Computer Science & Engineering from University of Engineering & Management, Kolkata, India. Presently he is working as Assistant Professor in Gargi Memorial Institute of Technology.

He has mentored the students group to win prestigious "NASA Space App Challenge" in the year 2019. He has also received the "Best Paper award" in 2018 for SCOPUS indexed Book Chapter in Springer. Sayan has published 3 SCOPUS indexed Book chapters and also presented his papers in reputed International Conferences such as IEEE in Las Vegas, America. His main research interests include Machine Learning, Deep Learning, Pattern Recognition, AD Hoc Network, Artificial Intelligence etc.

E-mail- sayan.cse_gmit@jisgroup.org.

Debika Bhattacharyya has got her B.Tech and M.Tech in Radiophysics & Electronics, Calcutta University and Ph.D from ETCE Department Jadavpur University. She has obtained National Scholarship twice in her academic carrier from Govt. of India. Her current research area includes Artificial Intelligence, Wireless Adhoc Network, Sensor Network etc. She has got 26 years of experience out of which 6 years of industrial experience. She has got award of Best Teacher in IEM in 2006 and 2014. Apart from India she has taught in Cambridge online city UK. She has acquired 2 AICTE funded and 2 DST funded projects. She is the "Eastern Zonal Lead" in a prestigious Pan India Project, "Making "Deep Learning and AI skills" mainstream in India to fulfil trilateral needs of entrepreneurship, Industry-academia partnership and application-inspired Engineering Research" funded by "Royal Academy of Engineering", UK (Rs. 3.3 crore) under the leadership of Bennett University. She is currently Dean-Academics and Controller of Examination in IEM.

E-mail- bdebika@iemcal.com.