International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-3, January, 2022

Intrusion Detection in Manet Through Machine Learning Approach

Sultanuddin SJ, Md. Ali Hussain

Abstract: ***Mobile ad hoc networks (MANETs) have evolved into a leading multi-hop infrastructure less wireless communication technology where every node performs the function of a router. Ad- hoc networks have been spontaneously and specifically designed for the nodes to communicate with each other in locations where it is either complex or impractical to set up an infrastructure. The overwhelming truth is that with IoT emergence, the number of devices being connected every single second keeps increasing tremendously on account of factors like scalability, cost factor and scalability which are beneficial to several sectors like education, disaster management, healthcare, espionage etc., where the identification and allocation of resources as well as services is a major constraint. Nevertheless, this infrastructure with dynamic mobile nodes makes it more susceptible to diverse attack scenarios especially in critical circumstances like combat zone communications where security is inevitable and vulnerabilities in the MANET could be an ideal choice to breach the security. Therefore, it is crucial to select a robust and reliable system that could filter malicious activities and safeguard the network. Network topology and mobility constraints poses difficulty in identifying malicious nodes that can infuse false routes or packets could be lost due to certain attacks like black hole or worm hole. Hence our objective is to propose a security solution to above mentioned issue through ML based anomaly detection and which detects and isolates the attacks in MANETs. Most of the existing technologies detect the anomalies by utilizing static behavior; this may not prove effective as MANET portrays dynamic behavior. Machine learning in MANETs helps in constructing an analytical model for predicting security threats that could pose enormous challenges in future. Machine learning techniques through its statistical and logical methods offers MANETs the learning potential and encourages towards adaptation to different environments. The major objective of our study is to identify the intricate patterns and construct a secure mobile ad-hoc network by focusing on security aspects by identifying malicious nodes and mitigate attacks. Simulation-oriented results establish that the proposed technique has better PDR and EED in comparison to the other existing techniques.***

Keywords: Machine Learning, MANET, topology, Mobility, Anomaly Detection.

I. INTRODUCTION

A.To Manet Security Challenges and Approaches

Manuscript received on December 21, 2021.
Revised Manuscript received on December 25, 2021.
Manuscript published on January 30, 2022.
* Correspondence Author
Dr. Sultanuddin SJ*, Department of MCA, MEASI Institute of Information Technology, University of Madras, Chennai (Tamil Nadu), India. Email: sayedjamalsultanuddin@gmail.com
Dr. Md. Ali Hussain, Department of ECE, KL Deemed to be University, Guntur (AP), India. Email: Alihussain.phd@gmail.com

The distinctive characteristics of MANETs [1,10,12,17, 19] with respect to decentralization, availability, flexibility and self-administration serves as a boon as well as bane as it draws attention from multiple sectors [14,15] to deploy in their operations along with inviting various types attacks (Fig 1) due to its vulnerabilities. Several researchers have recommended a variety of security mechanisms to detect and mitigate the effects of attacks on MANETs.

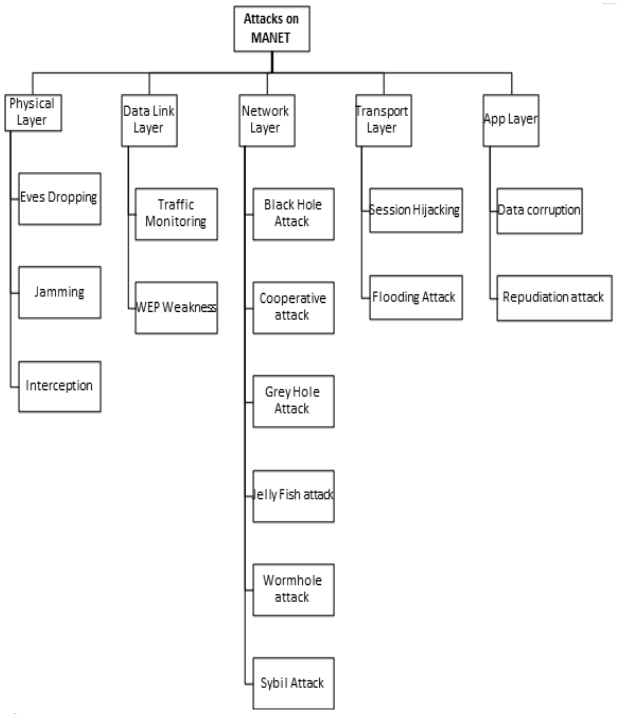


Fig 1: MANET Attacks

Cryptographic mechanisms [2, 3, 4, 8] offered certain merits by introducing a considerable delay in communication moreover it required the connection beforehand to maintain the data transfer between the nodes which is not practicable in Mobile ad-hoc networks, hence hybrid methods are required to enhance security in MANET as the nodes are open to various attacks in different layer of MANET (Table 1). For instance, some of the familiar and most commonly occurring attacks[13,17] are denial of service, eavesdropping, man in the middle, flooding, Sybil, worm hole spoofing, impersonation, black hole ,jamming and grey hole attacks etc. which targets specific layers. To some extent intrusion detection systems, encryption mechanisms,

spread spectrum analysis and firewalls can work towards detecting diverse type of attacks but the last decade witnessed a shift in network paradigm from cryptography to novel technologies like AI, machine learning and genetic algorithms.

Table 1:Security attacks in different MANET layers

Layers	Types of Attacks	Security Problems
Application	Repudiation and data modification	Detection and prevention of viruses,worms and malicious nodes
Transport	Session and traffic monitoring and hijacking,SYN flooding	Authentication and secure communication
Network	Jelly fish,Grey hole,worm hole,black hole attacks	Protection from ID spoofoing and securing routing protocols
Data Link	Traffic monitoring,resource consumption,location disclosures	Prevention of MAC disruption through link layer based security
Physical	Eaves Dropping,Message Interception	Prevention of DOS and jamming of signals

Intrusion Detection mechanism [10, 11, 21] corresponds to defensive strategy deployed in MANETs to examine and probe events that happens out of ordinary which comprises of several methods to detect abnormalities or anomalies in the network. IDS can be generally of three types- anomaly detection, misuse detection or signature oriented detection. Anomaly detection based mechanism can filter abnormal outlier nodes by evaluating them with regular normal patterns. A node is labeled as intruder if outlier is detected. On the other hand, misuse detection and signature-based detection relies solely upon saved signatures or patterns hence they cannot be utilized to spot innovative threats or attacks. Thus, anomaly based detection surpasses the other two in terms of its ability to handle novel scenarios like in MANETs ,which is known for its dynamic and open environment nature where nodes can connect and leave at any time in ad hoc fashion that makes them even more vulnerable to several possible attacks. The key intention is to recognize any malevolent activity prior to actual danger so that nodes in MANETs are endowed with the capability to filter the illegal and unauthorized entries. Since nodes are constrained of resources like power, storage etc., it creates an immense challenge in implementation of anomaly detection in real time applications. Machine learning methods facilitates in discovering diverse and novel threats along with vulnerabilities of the existing system. Configuration of ML techniques can be based on neural networks, fuzzy logic, genetic algorithms[22] or Bayesian network[21]. These technologies have turned into a remarkable alternative for security analysts as well as researchers to arrive at efficient and optimized solution for security enhancement in MANET environments. Therefore, this paper introduces a novel approach which can perform discovery, avoidance, forecast and alleviation of compromised nodes and secure the routes based on machine learning and clustering algorithm. The paper is categorized as follows: Section 1 gives a brief introduction to MANET and its security approaches. Section 2 provides some recent research literatures in relation to our study. Section 3 briefs about machine learning and its application in MANET intrusion detection. Section 4 explains the proposed method followed by simulated results in section 5. Study is concluded in section 6 with a scope for further research in future.

II. RELATED WORK

Following are some literature insights from some existing works related to the area of our research that has motivated towards studying this particular methodology to protect and safeguard MANETs from any possible hostile attacks in future. Distance based outliers (Knorr et al, 1998) were detected based on the estimation of distances of objects through an outlier factor represented as *OF: x* $\rightarrow$*O*. Similarly density (Breunig et al, 2000) based outliers were evaluated from input data in which several outliers were identified on the basis on their distribution. Outliers were generally identified in lower density regions as per this method. Fan et al (2003) offered a cross-feature analysis approach which aims to capture the correlation patterns present across the features in normal input data traffic. These patterns can be established as normal profiles which can then be utilized to detect anomalies. However, these normal profiles can be established only through initial training of input data and because of node mobility and dynamic topologies of MANET, they cannot be used to accurately represent the actual state of the current network. Lee et al (2004) used specification and statistical methods to recognize attacks in AODV through finite state automaton based detection of anomalous behaviors. Statistical learning algorithms and violation specifications were used to detect anomalous characteristics that showed temporal and statistical features. Chen et al(2006)observed that outliers could emerge from variety of sources like data inconsistency, environmental factors, software or hardware, can originate from node /network, statistical or knowledge based, distance/density oriented ,Markov/hidden Markov outliers etc., Hence to solve and identify outliers is to design a mathematical model based on data probability and statistics. Pooch et al. [2007] recommended an anomaly detection method which took into account of MANET's node mobility factor. During training stage, different mobility models, their routing activities at various mobility levels were gathered and link change rate at every level was computed. During detection phase, every node frequently estimated its present link change rate and opted for normal profile whose rate had the least Euclidean distance in comparison to current link change factor. Zhang et al (2010) recommended a statistical method where user oriented behaviors is studied by making use of certain measures. Regression based analysis was also utilized to detect the outliers when the system is in its running condition. Yang et al (2011) emphasized on Markov chain process in which discrete state spaces were described using temporal dependency between current and subsequent states.

Retrieval Number: 100.1/ijitee.C96790111322
DOI: 10.35940/ijitee.C9679.0111322
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Kato et al (2012) proposed anomaly detection based on dynamic updating of training data which requires the first set of data to be used as training data. Hybrid detection methods (Imani et al, 2015) were suggested where anomaly and misuse based detection methods were integrated to reduce the costs and reap the benefits of both the mechanisms. This approach also made use of hidden Markov chain model to maintain data transfer related history and to ensure security. In the same year Ram Mohan et al (2015) presented a clustering based technique to detect anomalies which made sure that the detected anomalies are genuine as the false alarm rates are low. Prasanna lakshmi et al (2019) put forward a method to enhance security features of MANET through anomaly-based intrusion detection which made use of ZRP, AODV routing protocols to discover the shortest route which comprises of attribute selection based on ID investigations of malicious nodes and recognizes new attacks through logical decision rules queried from rule database. Samanta et al(2020)too suggested a trust based secure routing mechanism which detected attacks like wormholes and black holes injected by malicious nodes in the network.The model was shown to reduce the power consumption and improve the efficiency.Veluswamy et al(2021)proposed an energy efficient trust factor based on AODV protocol which performs the task of isolating malicious nodes through dynamic estimation of power consumption and trust values as per the changing topologies and improves the performance of routing with the administration of AODV which minimises EED and PDR.

III. OVERVIEW OF INTRUSION DETECTION SYSTEM AND MACHINE LEARNING IN MANET

The primary goal of an intrusion detection system (IDS) is to identify threats or any malicious activities occurring in a isolated or in a network system through periodic monitoring of traffic. In case of MANETs [10,15]where mobile wireless nodes are dynamically self configured and hence IDS has become an essential component of nodes to equip the network with high intense security. Regardless of the merits with respect to high degree flexibility, scalability and extensive array of applications being accomplished through MANETs, the inherent vulnerabilities enhance the security related constraints. In order to securely employ MANET and exploit its accommodating and dynamic characteristics, highly reliable and robust security mechanisms are the need of the hour. However, avoidance of intrusion cannot possibly eradicate any potential intrusions and can only be made of use as the first level of defense against any future attacks. Recognition of intrusion through classification based procedures can effectively distinguish between normal and out of ordinary behavior and thus aids in detecting intrusions in MANET which can therefore be made a second level of defense that can serve as the foremost building block in communication. In wired networks all the traffic go through devices like switches or routers or gateways which facilitates the implementation whereas in MANET, absence of these devices and due to its open nature, any client can gain entry .Thus wired IDS techniques cannot be implemented on MANET directly. Generally IDS techniques that can be used on MANET is of 3 types namely[5,6,20]

- **Stand alone IDS**
  - IDS system runs on every node on MANET
  - Absence of collaboration between the nodes in the network
  - Local or global response is generated if an intrusion event occurs
  - IDS agent identifies and collects intrusion information locally
  - Effective only in flat networks not suitable for multi layer or complex networks.
- **Hierarchical IDS**
  - Network is fragmented into clusters and IDS is deployed in CH
  - The cluster heads act as a central point of information collection and monitoring of intrusions
  - Cluster head serves as both local as well as global IDS agent Suits multi layer and complex MANET network architectures
- **Distributed and cooperative IDS**
  - Every node is endowed with IDS agent who is accountable for detecting and gathering local as well as global responses and cooperates with other nodes in case of global detection and wide search scenarios.
  - Alert responses are raised by local or global agent based on detection of intrusion
  - If the collected evidence is uncertain then neighboring IDS agents cooperate in detecting global intrusion.
  - This system is also more suitable for flat network systems and cannot be applied for multi - layer based systems.

ML [16, 25] facilitates in easy summarization and visualization of input data which helps the security analysts to recognize vulnerabilities and flaws that exists in the current system. To enhance the rate of detection along with its compliance, several techniques of ML have been implemented to address intrusion detection related issues in MANET. These practices are frequently adopted to record the recent events and maintain comprehensive information with respect to several attack scenarios. The main categories of ML are

- Supervised learning algorithms
  - Training in the presence of a supervisor where data is trained to arrive at accurate or desired outcome. The supervised learning algorithm scrutinizes the learning data and generates an output in accordance to its discrete or continuous nature.
  - ANN,SVM,KNN, decision trees, Random forest ,linear and ensemble classifiers are the examples
- Unsupervised learning algorithms
  - Involves past experience based training on data learning, does not includes objectives or calculations based on predictions. Revolves around the problem of unmarked data discovering a secret structure where there is no specific objective

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- Examples are k-means clustering, hidden Markov models, genetic and fuzzy logic algorithms.
  - Reinforcement learning algorithms
- In this technique ,an agent is trained to learn in an interactive setting through trial and error based responses collected from its actions and incidents
- Deep Q-Learning, SARSA , Deep Adversarial Networks, A3C,TD are the examples

IV. PROPOSED MODEL

The proposed model has been designed by using machine learning based on hierarchical IDS and reinforcement learning model which makes use of decision tree algorithm to enhance the precision and performance of intrusion detection in MANET through anomaly detection based learning process. At the time of transmission, the constraints with respect to dropping and delaying of packets can happen due to traffic congestion and collision along with the non-availability of link due to exposed and hidden terminal issues. This in turn will generate false alarms due to mistaken identification of normal as malicious node pattern in the MANET environment. To avoid the aforementioned issue, and to handle the dynamic network topology and mobility of nodes, the machine learning system deployed is decision trees. Following are the main components of our model namely whose flowchart is presented in Fig 2

- **Cluster head/ IDS agent**: Responsible for performing intrusion detection through learning process and conducts examination and investigation of MANET devices to validate their behavior through cooperation between input and output components which employs decision tree based reinforcement learning mechanism**.**
- **Input component**: Parameters collected by nodes which acts as the input to IDS agent
- **Output component**: Detected patterns or behaviors of all the nodes by IDS agent
- **Intruder**: Device involved in hacking, modification and damage of data packets resulting in reduced efficiency of the system

The working method of the proposed model is as follows

- MANETs are set up with an intruder; attacker and a packet dropper produce false data packets. The data transmission is instigated by the source node and the path discovery process is implemented.
- All the nodes perform data transmission through request forwarding and receiving system. Route replies are created by targeted destination nodes and packets are forwarded by in-between nodes until source node is reached. Once route is discovered data packet forwarding is taken care by source and in-between nodes.
- Node monitoring is performed by cluster heads equipped with IDS, which keeps track of requests and replies and performs physical layer eavesdropping to monitor reception and forwarding counts of data packets. The false packets generated by the nodes are scrutinized by evaluating the packet size and initiates the detection process through reinforcement learning based decision tree algorithm (Algorithm 1).
- Attributes such as packet generation, drop rate, energy loss of each node for every data transmission, signal strength, data and control message forwarding ratios, reliability between original packet and dummy packets along with link aspects like occupancy factor, transmission probability, collision rate, error rate are estimated to discriminate between traffic congestion and malicious behavior.
- Q-learning is used to perform the mapping of states to corresponding actions whose values are estimated as Q (S_t; A_t) which represents the state and action pair which is updated in accordance to the equation
- $\alpha\, Q(S_t; A_t) = \mathcal{E}[R_{t+1} + \varphi \max_{A_{t+1}} Q(S_{t+1}; A_{t+1}) Q(S_t; A_t)]$ (1)
- where $\mathcal{E}$ is the learning parameter$0 \leq \mathcal{E} \leq 1$, t denotes the current time, R_{t+1} is the reward collected at time t + 1, S_t is the state, A_t denotes the action performed at time t, φ manages the reward and return ratios between present and future states. In our proposed model, decision tree has two types of nodes namely decision and child nodes. A decision node represents the decision made about a particular MANET node to determine which node is selected to route the packets.
- Each child node stores the calculated values for its regions in the corresponding state space. In Q-learning every child node stores a single value for every action along with rules to decide if the node should be partitioned if the node is malicious. The decision tree initiates with single child node with the implementation of the algorithm information is updated in record list which gets updated frequently.
- If a malicious node is encountered based on the trust factor and other input criteria, a decision is made to determine if the packet has to be forwarded or partition should be made to surpass the intruder. If partition is made, then the corresponding route is updated and a new node is created to replace the child node, and two child nodes are attached to the parent node after removing the old child node. In this way, the decision tree grows from the root towards down by continuously partitioning and discovering the node based on decisions.

DECISION TREE ALGORITHM FOR REINFORCEMENT LEARNING

1. Obtain input parameters and reward R_t for time *t*.
2. Apply input values to locate the child node whose state is S_t.
3. Select either the appropriate action with maximum value of Q (S_t; A_t) or a small pr for random action.
4. Incase appropriate action is selected then calculate $\alpha\, Q(S_{t-1}; A_{t-1})$ and update $Q(S_{t-1};$
5. Append $\alpha\, Q(S_{t-1}; A_{t-1})$ to the record list for child node corresponding to S_{t-1}.
6. Choose if S_{t-1} should be divided into two by investigating the record list for S_{t-1}.
7. Incase if record_ list _length < record_ list _min size then partition := F
8. Calculate average μ and standard deviation σ of $\alpha Q(S_{t-1}; A_{t-1})$ in the record list
9. If $|\mu| < 2\sigma$ then partition := T else partition := F
10. Perform partition, if needed or update the values of R_t , A_t and S_t to be utilized fo during next iteration.
- 11.Return A_t

Algorithm 1: Decision tree based reinforcement learning

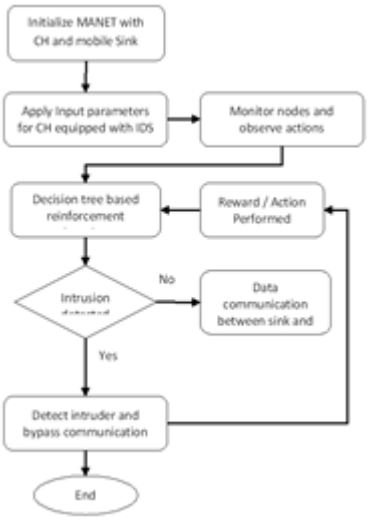


Fig 2: Flowchart of the proposed system model

V.SIMULATION AND RESULTS

Simulation process of the proposed model is performed with NS2.33 network simulator where a location of 2000*2000 m^2 is constructed for MANET experiments with communication support for multi hop wireless communications of bandwidth 4Mbps where mobility of nodes is set at random pace with speed of 5m/s and the transmission range is around 500m. Traffic type is CBR and the size of the packet is 1024 bytes. The proportional results observed through three different test conditions where varying the nodes count (30 to 150) with the difference of 30 nodes in every simulation. Second test condition is implemented by utilizing different packet generation rates (0.1 to 0.5). And third condition is experimented through setting the simulation time (30 s, 60s, 90s, 120s, and 150 s). Results are evaluated by analyzing them with existing detection approaches like Naïve Bayes Classifier and Genetic algorithm to validate the performance of the proposed model. The simulation attributes and the corresponding values are represented inTable2

Table 2: Simulation attributes

SIMULATION ATTRIBUTES AND VALUES	
Nodes count	30 to 150
Speed	5m/sec
MAC	MAC 802.11
Network Area	2000*2000m²
Range of transmission	500m
Connection type	UDP
Traffic type	CBR
Traffic interval	0.2sec
Mobility type	Random
Bandwidth	4MBps
Packet size	1024 bytes
Time taken for simulation	100 seconds

Following are the performance metrics taken into account to evaluate the system performance in detecting the malicious nodes and safeguarding the security of the MANET.

Packet delivery ratio

The packet delivery ratio (PDR) which gives the information about the number of packets successfully delivered is illustrated in Fig 3 which increases with increase in packet generation rate and shows that packet has been successfully received by destination node and our proposed model (IDS-RL) outperforms the other two Genetic Algorithm (GA), Naïve-Bayes Classifier (NBC) for as far as intrusion is handled.

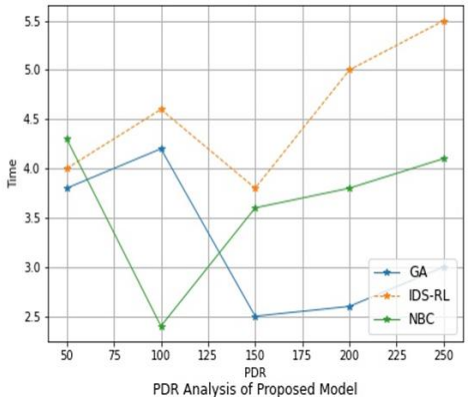
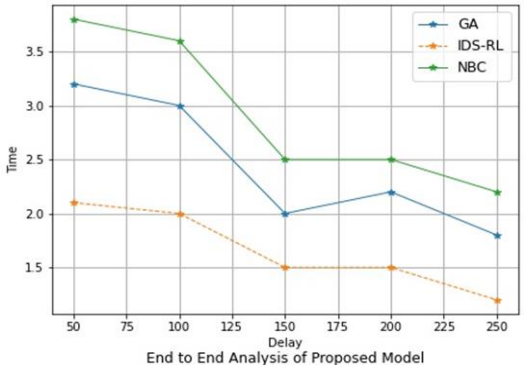


Fig 3: PDR analysis of proposed model

End to End Delay:

The average end-to-end delay is presented (Fig 4) with varying number of nodes. As illustrated in the graph, by varying the number of nodes, the end-to-end delay has been minimized. Through efficient clustering mechanism and IDS monitoring delay is reduced and PDR is enhanced and it can be seen that the proposed model provides enhanced results when compared to existing approaches.



VI. CONCLUSION AND FEATURE ENHANCEMENT

MANET environments are known for their open nature where nodes are free to join and leave at any time and communicate with each other in the absence of any central authority. This unconditional freedom of movement of nodes in the network poses serious security issues as the routes established for data transmission are neither stable nor reliable which could cause concerns in sensitive real time applications where security must be the priority.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Hence proposing a safe and robust model for MANET environment without compromising on the underlying cooperative nature is a huge challenge. Machine learning algorithm has been applied in the proposed model to opt for the reliable and trust worthy neighboring node for data transmission in the MANET. The simulation conducted in NS2 demonstrates the merits of this recommended model in comparison to existing strategies. Thus, the key focus of this contribution in the selection of a trusted node for transmission through identification of malicious nodes and differentiating them from normal nodes and designing a secure network has been accomplished. Future work is oriented towards selecting the decision boundaries through exploration of some alternative techniques with a perspective of characterizing the working of approach that would provide good learning performance and meets our QoS based requirements in a more reliable convergence with lower memory requirements and better scalability in large complex MANET environments.

REFERENCES

1. Ali Dorri, S. R. (2015). Security challenges in Mobile Adhoc Networks: A Survey. International Journal of Computer Science & Engineering Survey, 6 (1).
2. Bharathisindhu P, S. B. (2018). An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network. cluster computing, The Journal of Networks, Software Tools and Applications
3. D, S. Intrusion Detection in Mobile Adhoc Networks. Texas,A M university.
4. Hasswa A, Z. H. (2005). Routing Gaurd:An Intrusion detection and Response system for Mobile Adhoc Networks. IEEE International Conference, (pp. 336-343).
5. Liu K, D. J. (2007). An Acknowledgement Based Approach for the detection of Routing misbehaviour in MANETs. Mobile Computing (pp. 536-550). IEEE Trans.
6. Marti S, G. T. (2000). Mitigating Routing Misbehaving in Mobile Adhoc Networks. Mobile Computing, (pp. 255-265).
7. Miranda H, R. L. (2001). Preventing selfishness in open Mobile Adhoc Networks. Seventh CaberNet Radicals Workshop.
8. Nadiammai G.V, H. M. (2014). Effective approaches towards Intrusion Detection system using Data Mining techniques. Egyptian Informatic Journal , 37-50.
9. NanKang, E. M. (2010). Detecting Misbehaving Nodes in MANETs. iWAS . Paris,France.
10. Ramasamy Murugan, A. S. (2013). A TImer based Acknowledgement scheme for Node Misbehaviour Detection and isolation in MANET. International Journal of Network Security , 182-188.
11. Saravanan S, C. R. (2005). Intrusion detection system using Bayesian approach . International journalof engineering Innovtive Technology , 108-116.
12. Sheltami T, R. A. (2009). video transmission enhancement in presence of misbehaving nodes in MANETs. International journalof Multimedia systems , 273-2
13. Sheenu Sharma and Roopam Gupta,(2010) ,Simulation study of Black hole attack in Mobile Ad hoc Networks,‖ Engineering science and Technology
14. M.I.M. Saad and Z.A.Zukarnain, (2011)Performance analysis of random-based mobility models in MANET routing protocol,‖ European Journal of scientific Research
15. Jayakumar.G and Gopinath.G, (2013), Ad hoc Mobile wireless network routing protocol-A Review,‖ International journal of computer science, 3(8), pp.574-562.
16. Buttyan,L. and Hubaux J.P, (2009),Security and cooperation in wireless networks
17. S. Sharma,(2013).An Effective Intrusion Detection System for Detection and Correction of Gray Hole Attack in MANETs,‖ Internantional Journal of Computer Appllications, vol. 68, no. 12, pp. 1–5, 2013.
18. S. Marti, T. J. Giuli, K. Lai, and M. Baker,(2000),Mitigating routing misbehavior in mobile ad hoc networks,‖ Proc. 6th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom ’00, vol. 7, pp. 255–265, 2000.
19. D. J. Liu K,(2007),An Acknowledgement Based Approach for the detection of Routing misbehaviour in MANETs,‖ Mob. Comput. IEEE Trans, vol. 6, no. 5, pp. 536–550, 2007.
20. Nan Kang, Elhadi M.Shakshuki, Tarak R.Sheltami,(2010), Detecting Misbehaving nodes in MANETs‖, iiWAS2010 proceedings security issues, pp.216-222,2010.
21. ShubhangiS.Gujar and B.M.Patil, (2005), Intrusion detection using Naïve Bayes for real time Data,‖ International journal of advances in engineering and technology
22. R. Desale, Ketan Sanjay and Ade, (2015),Genetic Algorithm based Feature Selection Approach for Effective Intrusion Detection System,‖ 2015 Int. Conf. Comput. Commun. Informatics, 2015.
23. Bharathisindhu.p., and Selva Brunda.S,(2018),An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network.‖ Cluster Computing, January 2018. Springer International Publishing. DOI: 10.1007/s10586-018-1745-7.
24. KanikaBawa, Shashi B.Rana, (2015), Prevention of Black hole attack in MANET using Addition of genetic algorithm to Bacterial foraging optimization,‖ International journal of current Engineering and technology, vol.5,No.4, Aug 2015.
25. Baskar.M, Gnansekaran.,(2017),Developing Efficient Intrusion Tracking System using Region Based Traffic Impact Measure Towards the Denial of Service Attack Mitigation”, Journal of Computational and Theoretical Nanoscience, Volume No.14, Issue No.7, pp: 3576-3582, ISSN: 1546-1955 (Print): EISSN: 1546-1963 (Online) , July 2017.

AUTHORS PROFILE

Dr. Sultanuddin SJ, working as Assistant Professor in Department of Master of Computer Applications. MEASI Institute of Information Technology. Completed his PhD in Satyabhama University. His area of interest is Networks, Database Management, and Software Engineering. Completed MCA and M.Tech IT., He has Published five scopus journals one sci journal and one each in national and international journal. Email: sayedjamalsultanuddin@gmail.com

Dr. Mohammed Ali Hussain, working as Professor in Department of Electronics and Computer Engineering, KLEF Deemed to be University, Guntur Dist., Andhra Pradesh, India. He has received 5 National Awards and 2 International Awards for his research contributions in various International Journals (Scopus & SCI). He is Editorial Board Member & Reviewer of various International Journals. He has published 6 patents to his credit and produced 3 PhD’s under his supervision. His area of Interest includes Wireless Networks, Mobile Ad hoc Networks and Web Security. He is a member of various professional bodies FISEEE, ASDF, UACEE, IACSIT. Email: alihussain.phd@gmail.com