International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 07 | July 2022 www.irjet.net p-ISSN: 2395-0072

Performance Analysis in MANET Routing Protocol using Machine Learning Algorithm for Data Security

Madhu M S [1], Dr. Chandrakala V [2], Praveen K B [3]

[1] *M.Tech Student[DCN]*
Department of Electronics and Telecommunication, Dr. Ambedkar Institute of Technology, KARNATAKA, INDIA

Abstract - Mobile ad hoc networks (MANETs) only have individual sidekicks and lack an edge. This article demonstrates rigorous convention-directing testing for MANET. The testbed running on the Linux platform is shown on mobile PCs. For outline, advancement speed, and the number of hops that affect steering judgment, various limitations are excavated. Once again, two performances are chosen to be coordinated for the testbed evaluation. The main display is referred to as BABEL and is a computation for coordinating partition vectors. The enhanced interface state directing convention (OLSR), which is regarded as a visionary controlling show, is the alternative. A multi-bounce download of archives with distinct sizes was the application scenario. The goal is to analyzer what different bobs signify for holdback and exchange speed. The problems show that OLSR performs better in terms of the outcome. Babel, however, has lesser deferral and is hasty with conjunction.

Key Words: MANET, wireless communication, Routing Protocols, transmission delay and packet delivery ratio, energy consumption.

1. INTRODUCTION

The dynamic penetration of remote connections (3) Mobile or remote ad hoc network is a cutting-edge technology that enhances the tendencies to develop positive strikes or solid organization. Does not count on design (2). The hits included in this mobile network or remote ad hoc network are not resolved in any way; Instead, they strike freely and extend the connection to a nearby device via a remote without the need for a centralized entity to keep them pointed in the right direction. Because it is moving, it beats gradually and quickly (9). Because of its outstanding features, mobile ad hoc networks create many routing challenges because strikes in the ad hoc network occupy a portion of the hosts and switches needed to conquer all data (2). Therefore, routing calculation plays an important role in MANET Rebar design. (3) These intriguing features make MANET popular in a wide variety of missions, including military governance, marine science, clinical fields, attractive departments, area regulation and recovery missions. As part of the research, philosophies were applied to traditional networks such as

Table-Drive, On-Demand, Situation-Centric, Progressive, Senseless and Multipath (1) using comprehensive data for traditional methods such as B (12). In order to improve the organization's existence, it is necessary to lessen or change the way that portable ad hoc networks are managed since the drawbacks include low power inclination. to simplify the process of transmission while maintaining calmness. Finalizing the steering setup that generates a portable hello correspondence that is occasionally communicated along with the knocks speed to decrease traffic and outpouring in the organization (5), the directing hybridizing two or different styles were also used (13), (14), and (15) in risking a more available framework, to limit start to finish confinement and the memory and power usage. A sample of the steering options for the MANET are shown in fig. 1 below.

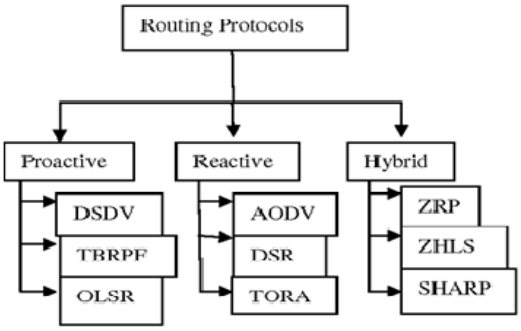

Fig-1: Routing protocol in MANET

Every single style examined up until this point used methods to enhance organizational life by reducing energy consumption and reducing restrictions while looking into the quickest possible means of information transmission, but they all failed to gather information on how to maintain a constant means of communication.

Therefore, the suggested framework makes use of the type of machine education, the supporting learning for portability vaticination of knocks corresponding to the objective taking advantage of the knocks from the data that could support in laying out the most constrained course alongside the steady way.

1.1 Security Approaches in MANETs:

The decentralization, tonal operation, and other intriguing features of the MANET attract effective attacks within the organization. Over the past ten years, a variety of security measures have been introduced to repel attacks and mitigate

their by-products. A wide range of these methods appear under the highest security standards on MANETs, built on a cryptographic approach. A complex framework of functionality was approved in 1999 for the use of limited ciphers for certification processing on specifically designated networks. Some of the strikes carried out the work of the servers in the proposed framework, but most of the strikes stole the chief part. In addition, SAODV - Comprehensive Understanding of AODV - (4) was introduced. The proposed system uses computerized hash chains and signatures for cryptographic security on designated networks. Several cryptographic systems have been set up on central authority to push tools for verification reasons (5) (6) (7). (8) However, some other approaches, such as the trust model of the PGP network (9), changed the origin of central management (10). As a result, the authentication process involves a series of tools stored at its ends. In these styles, the real group is ready to store their tools. In writing, it was noted that the ciphers introduced critical limitations in communication and that a pre-link between the hits must be maintained, which is not achieved in casual meetings. Therefore, experimenters have used a wide range of hybridization designs to improve the security of the MANET. Strikes on MANETs are subject to a variety of attacks, such as dynamic and open attacks. For example, some examples of common attacks are Power-Challenging, Man-in-the-Middle, Flooding, Mocking, Pantomime, Dark Opening, Opening Scoring Attacks, etc. Fine intercept detection frameworks are used in the literature to describe a wide variety of attacks.

In short, various cryptographic tools have been used in the past to highlight the security features of the MANET, but over the past 10 years there has been a change in the way we view networks as new developments such as machine learning, deep learning, and artificial intelligence. and hereditary calculations became a key decision. Experimenters on MANETs risk practical, security-enhanced results. This study provides recent developments that have proven effective in providing safety outcomes. Included in the Excellent Safety Guidelines based on Machine Perfection, as well as the detection, prevention, adoption and mitigation of penetrating strikes.

1.2 Machine learning-based security solutions:

Sending emails and signing contracts, for example, would be impossible without adequate security measures in place.

When creating sensitive software, it's crucial to keep in mind the organization's fundamental security pillars.

A prediction model may be built utilizing manufacturing data for certain attack scenarios and evaluated with the remainder of the test data using AI approaches. The quality of the learning model is scrutinized in light of the precision with which new attack designs may be detected. The hubs on the MANET are more vulnerable to various types of attacks such as floods, DoS attacks, dark openings, wormholes, dim openings, etc. due to the company's open environment. Hubs on the MANET also display multi-echo correspondence, meaning that the source hub transmits packets to several intermediate hubs before sending them to the target hub. All communication depends on the cooperation of the interlocutor. To prevent packets being diverted to any malicious or malicious hubs within the company, it is important to determine the reliability of the hubs as part of security efforts. To improve security in the organization, several confidence assessment approaches have been proposed in the literature. The classmates shown in Figure 1 can be used to separate security devices on MANETs. In addition, ML plays an important role in improving the security of many specially designed networks. In MANETs, different ML computations can be used to isolate interruptions and clear attack strategies. To improve the security features in the company, many intellectual frameworks are other written proposals. The following three obvious security areas are discussed in MANET using ML-based approaches:

2. Related works:

Hua Liang, Yanh Hong Shang et al.,[24] proposed to study the DTN routing protocol for a vehicle-specific network based on machine literacy. MANET incorporates the Vehicle-Mounted Tone-Arranging Network into this architecture. It is between good correspondence equipment and off-road vehicle. It serves as the hub for all street vehicles and offers multi-horsepower remote controls and the ability to exchange data with other vehicles.

According to Dr. M. Duraipandian's [25] proposed routing method based on reinforcement algorithm by establishing the shortest path for the mobile ad hoc networks evaluating the parameters like throughput, packet delivery ratio etc.,

Rober a Sowah et al.,[12] presented intrusion detection systems using +e ANN classifier algorithm for network-varied traffic conditions and mobility patterns in multiple attacks which offers a productive and less expensive to perform MITM attacks.

Fig-2: MANET routing

3. PROPOSED SYSTEM:

3.1 Routing using Reinforcement Learning in Mobile Ad hoc Networks

The steering is a crucial component of a flexible ad hoc network, therefore the suggested system makes use of supporting advancing to route packages from the source to the target. When the lead includes the assurance of the detainment derived from the knocks readily available alongside the efficient transmissions of each bunch, the supporting learning selects the knocks based on the upsides of the direct. The most effective transmission is defined into a group using the k-implies bunching, which is not completely fixed with minimal restriction. Based on its price, the appropriate gathering is selected from the range of available gatherings. The best group selection is followed by choosing the nearby hitch for the coming leap, the group with the closest distance to the goal is selected to be the approaching bounce, and condition (5) provides the method used in group selection.

As a result, the group is referred to as a direct, and the group's worth is determined on the costs of the knocks. The quickest approach is then established by selecting kicks that are as close to the goal as possible. These two criteria assess the worth of the groups based on the quantity of effective transmission (succtrans) and the confinement of the transmission. (6) and (7) (delay trans).

$Delay_{trans} = A_s*(re_t= (v *MIN value).$ 1

However, arithmetic helps us to identify the fastest way to lose relevance as strikes are far from their intended location. Therefore, in the proposed course, support will also be used to assess the conditions of group flexibility to disassemble the blows.

3.2 Protection against hacking:

By keeping an eye on all data pertaining to that particular parcel, we are sustaining USOR in this module. Since the parcel in this module is linked by a recognized stoner's agreement, other groups cannot tell the information about that bundle apart.

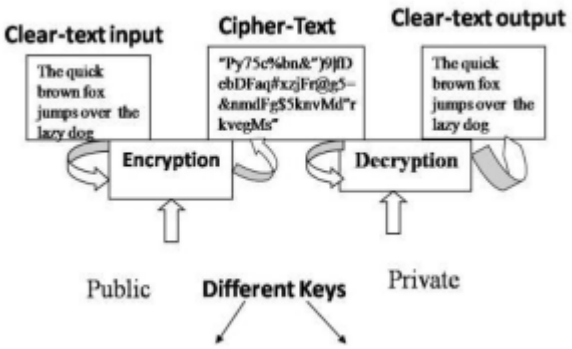

Fig-3: Security Block diagram

This module has a fake to authorize USOR while safeguarding all information included in the express bundle. In this module, only approved addicts are allowed to possess the bundle; attractive knocks cannot vouch for its contents. To further ensure safe communication, we added a sophisticated hand architecture to this. We can use cryptosystem design to create advanced signs. For a support wise meaningful cryptosystem, there are four cycles that are clear and essential.

a) Decrypting an encrypted communication reveals the precise original information

$D (E (M)) = M$ 2

b) Reversing the process still returns M:

$E (D (M)) = M$ 3

c) E and D are simple to compute.

d) You cannot just deduce D from E since E's openness does not yield D's concealment.

Suppose e, d and n are positive integers where e and n serve as the encryption key and d and n as the decryption key and n = pq.

To get C, for reading the code cycle, we now monitor the similarity by increasing the nth power scale. To get M again, we also translate C by increasing the power factor dth n. We officially get these coding and decoding equations for E and D.

$C = E(M) = M^e \bmod(N)$ 4

$M = D(C) = M^d \bmod(N)$ 5

3.3 Algorithm:

1. Source communicates course demand (RREQ) to the capitals of its neighboring countries and locates the course to thing.

2. Capitals truly examine their instructing table, and if no course is present, they reassign RREQ correspondence to their neighbors.

3. The process is repeated until the request reaches the object and the object responds to the source in a direct manner.

4. Eventually, the source will determine which sections of the proposed path are closest to them and forward channel request (CREQ) communication to the capitals and requests that their area deals with.

5. Capital cities react with channel reply (CREP) messages and provide information about their regional bearings to the source.

6. Source discovers the travel time (RTT) required to get the CREP, and whenever it is determined that RTT is more obvious than actual respect, it attests to the entry's proximity.

7. When the chosen association length is more than the actual length, wormhole capitals are identified. By and large, source figures interface length of associations existing in the way.

8. Source educates all other meccas to refrain from communicating with related wormhole capitals.

Position-Aware Services: Six Automatic Call Moving, Position-Sub-Par Turn Companion, Report Position Unambiguous Organizations.

4. Result and Discussion:

To demonstrate its feasibility and the short path that has been established, the proposed framework was tested using the Enterprise Test System II device. The proposed framework, which will form a stable path for a flexible temporary grid, is estimated to have 100 to 500 strokes, 100 joules of first force, 100 seconds of breeding season and 2500 * 400 square meters of recreational space. The proposed framework is comparable to previous models of the thin-film method, which is more limited for ad hoc networks (11) and shortens the life expectancy of the shorthand calculation method based on the firefly (9) to increase the life expectancy and transport life, based on the firefly (9) to demonstrate the increased viability of the suggested foundation for effective mail.

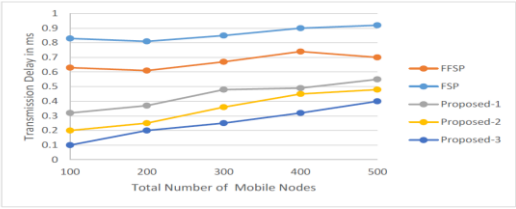

Fig .4 Delay in Transmission

Chart-1: delay in transmission

The proposed approach and the other two methods, vague shortcut determination for temporary mobile networks and the firefly algorithm for finding short paths for mobile networks, will be evaluated based on the above simulation result for transmission delay.

The built method is stable and due to some failures and diversion due to route instability, the proposed technology shows that it has less delay than the current one.

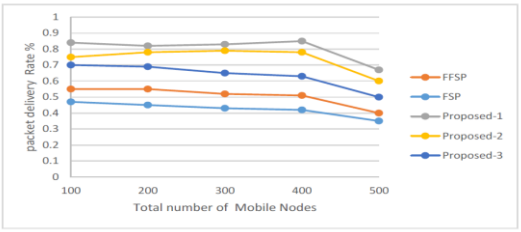

Fig.5Packet Delivery Rate

Chart-2: packet delivery rate

The simulation results above illustrate the rate of packets sent using the suggested strategy and the conventional method. Using reinforcement learning to build a consistent short route results in a 35% improvement in packet delivery. which has the effect of comparing the proposed method to the opacity (FSP) based shortcut and 28% method compared to the standard.

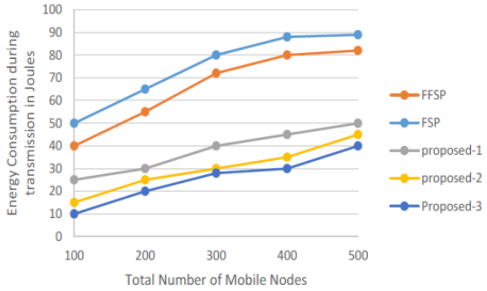

Chart-3: energy consumed during transmission

The simulation's findings on how much energy is used by the suggested approach and the standard method as they transmit packets from source to destination. The proposed

method demonstrates to have a significant amount of energy savings due to stable connection established, avoiding the circumstances of the rerouting protocol and links failure, even though all three methods have a limited energy consumption due to the establishment of the shortest path from the source to the destination. The simulation's findings on how much energy is used by the suggested approach and the standard method as they transmit packets from source to destination. Due to the establishment of the shortest path from the source to the destination, all three approaches have a restricted energy usage. the proposed solution avoids the circumstances of the rerouting protocol and connections failure and demonstrates a significant amount of energy savings thanks to the stable connection formed.

5. CONCLUSIONS

This study provides an honest evaluation of MANET routing protocols for data dissemination and optimal guidance. Examines the OLSR and Babel separation guidelines for output, execution and stability. On MANET PCs, these two preemptive heuristic conventions are frequently used. Our evaluation and research is based on testing with different hub portability settings and traffic volumes. Provided clear 10-axis results by implementing our unique setup routing convention with variable portability and traffic loads. Babel is considered to be the least resource in terms of using resources such as memory and handling.

Additionally, the Routing Update component specifies how to update chassis changes by sending control traffic as carrying routing if a link is found with remote systems that are large-scale or multi-echo routing. In such cases, the OLSR is considered superior to the Babel, and this arises because the OLSR has its entire cyclical temporal role in directing the sending and updating of structural elements, as Babel considers updating the course on a case-by-case basis. Due to Babel's actions, OLSR could not be compared to Babel in terms of joining strength or coupling capacity. However, the substantial cost of the routing agreement makes this babel reproduce an extra cycle and does not properly control traffic.

REFERENCES

[1] Goyal N and Gaba A, "A new approach of location aided routing protocol using minimum bandwidth in mobile ad hoc network", *published in International Journal of Computer Technology and Applications*, pp. 653-656, vol 4, ISSN:2229-6093, 2013.

[2] Popli R, Garg K and Batra S "SECHAM: Secure and efficient cluster head selection algorithm for MANET", *proceedings in IEEE International Conference on Computing for Sustainable Global Development*, pp. 1776-1779, volume 2, 2016.

[3] Kamboj P and Goyal N "Survey of various keys management techniques in MANET", *published in* International Journal of Emerging Research in Management and Technology, ISSN: 2278-9359, Volume-4, pp 176-178, 2015.

[4] Zapata M G and Asokan N "Securing ad hoc routing protocols WiSE", *Proceedings in ACM workshop on Wireless security*, pp. 1-10, 2002.

[5] Capkun S, Buttya L and Hubaux J P "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", *published in IEEE Transactions on Mobile Computing*, pp. 365-455, vol .2, 2003.

[6] Hamza F and Vigila S M C, "Review of Machine Learning-Based Intrusion Detection Techniques for MANETs", Proceedings in international conference in Computing and Network Sustainability, pp. 367-374, 2019.

[7] Bose S, Bharathimurugan S and Kannan "A Multi-layer intergraded anomaly intrusion detection for mobile ad hoc networks", *Proceedings in IEEE International Conference on Signal Processing Communications and Networking*, pp. 360–365, vol.11, 2007.

[8] Cabrera J.B.D,Gutirrez C, and Mehra R.K, "Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad hoc networks",Information Fusion 9 ,issue 1, pp. 96–119, vol.9,2008.

[9] Moradi Z, Teshnehlab M and Rahmani, "A Implementation of neural networks for intrusion detection in MANET", *Proceedings in International Conference on Emerging Trends in Electrical and Computer Technology*, Vol. 5, pp. 625-724, 2011.

[10] Lalli M and Palanisamy V "A novel intrusion detection model for mobile ad-hoc networks using CP-KNN", *published in International Journal of Computer Networks and Communications*, Vol 3, Issue 4, ISSN: 2319 -1953, (Impact Factor: 0.654)2014.

[11] Sebopelo R, Isong B and Gasela N "Identification of Compromised Nodes in MANETs using Machine Learning Technique", *published in International Journal of Computer Network and Information Security*, Vol.1, pp. 1-10, 2019.

[12] Sowah R A, Ofori-Amanfo K B, Mills G A and Koumadi K M, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)", *published in Journal of Computer Networks. and Communications*, vol**,** https://doi.org/10.1155/2019/4683982 pp 1-15, 2019.

[13] Goyal N, Sandhu J K, Verma L, "CDMA-Based Security Against Wormhole Attack in Underwater Wireless Sensor Networks", *published in Advances in Communication and*

Computational Technology Lecture Notes in Electrical Engineering, , pp 829-835, 2021.

[14] Patel M, Sharma S and Sharan D, "Detection and prevention of flooding attack using SVM", Proceedings *in International Conference on Communication Systems and Network Technologies,* pp. 533–537, 2013.

[15] Wenchao Li, Ping Yi, Yue Wu, Li Pan and Jianhua Li, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network", *published in Journal of Electrical and Computer Engineering*, pp 1-8, 2014.

[16] Patel N J and Jhaveri R H, "Detecting packet dropping misbehaving nodes using support vector machine (SVM) in MANET", *published in International Journal of Computer Applications,* vol. 122, pp 1-7, 2015.

[17] Elwahsh H, Gamal M, Salama A A and Henawy I M, "A novel approach for classifying MANETs attacks with a neutrosophic intelligent system based on genetic algorithm", published *in International journal of Security and Communication Networks*, pp 1-10, vol.3, 2018.

[18] Shams E A and Rizaner A, "A novel support vector machine-based intrusion detection system for mobile ad hoc networks", *published in International Journal in Wireless Networks*, vol.24 pp.1821-1829, 2018.

[19] Suma R, Premasudha B G and Ravi R V, A novel machine learning-based attacker detection system to secure location aided routing in MANETs, *published in International Journal of Networking and Virtual Organisations*, pp.17 – 41, vol.22, 2020.

[20] Damiani E, Vimercati S.D.C.D, "Samarati P A wowa-based aggregation technique on trust values connected to metadata", *published in Electron Notes Theory Computer Science*, pp. 131–142, 2006.

[21] Jinarajadasa G, Rupasinghe L and Murray I,"A reinforcement learning approach to enhance the trust level of MANETs", *proceedings in National information Technology*, pp. 1-7 , 2018.

[22] Jinarajadasa G M and Liyanage S R, "A trust based advanced machine learning approach for mobile ad-hoc network security", *proceedings in International Conference on Advances in Computing and Technology,* pp. 1-7, 2019.

[23] Popli R, Juneja V, Garg K and Gupta D V, "Fuzzy Based Trust Evaluation Model for Enhancing Security in MANETs" *published in International Journal of Engineering and Advanced Technology*, vol 8 , pp. 506-510, 2019.

[24] Hua Liang, Yanh Hong Shang et al Study on DTN Routing Protocol of Vehicle Ad Hoc Network Based on Machine Learning Volume 2021, https://doi.org/10.1155/2021/7965093

[25] Dr. M. Duraipandian's performance evaluation of routing algorithm for MANET based on the machine learning technique Journal of trends in Computer Science and Smart technology, vol 01,pp 24- 35, 2019.