ISSN: 2093-5374 / E-ISSN: 2093-5382

Development of a Lexicon for Manets to Enhance Performance and Security

T. Yogesha[1*], and Dr.S.N. Thimmaraju[2]

[1*]Assistant Professor, Department of CS&E, VTU PG Centre Mysuru, Karnataka, India.
yogesh@vtu.ac.in, https://orcid.org/0000-0002-7662-6064

[2]Professor. Department of CS&E, VTU PG Centre Mysuru, Karnataka, India.
thimmaraju_sn@vtu.ac.in, https://orcid.org/0000-0001-5090-8277

Received: November 06, 2024; Revised: December 18, 2024; Accepted: February 07, 2025; Published: March 31, 2025

Abstract

Mobile ad hoc networks is a challenging area of engagement since these networks are dynamic and completely without a definite structure. The lexicon, as a MANETs notion, plays an indispensable role in establishing smooth communication and coordination among the network nodes. The abstract's intention is to give an in-depth outlook for the role of lexicon in MANETs, and then it gives the central points of its importance in the connection of not only different communication protocols but also routing algorithms and security mechanisms. The abstract is mainly about the very basics of lexicon in relation to MANETs, with a more particular accent on how it enables strong communication if there is no fixed structure behind it. Suppose you also deal with the problems and possibilities of the so-called lexicon, which is the integration of lexicon technologies, such as unpredictable mobility and resource limitations. We'll also see the application of the lexicon in MANETs in the future. This is an approach based on the nominal size of the items focused on lexicon technology. For example, smarter routing protocols, QoE/QoS adaptation, and a defence guarantee for the protected message are among the key features that should be addressed through the application of lexicon technology in MANETs. The paper will review the current research work being conducted and present future directions for lexicon-driven approaches to optimize the performance of MANETs and make them more resilient to the variation of their operational environment.

Keywords: MANets, Security, Lexicon, Performance Metrics, Packet Exchange.

1 Introduction

The mobile ad hoc networks domain is the community of these kinds of networks, and the efficiency and reliability of the routing process are of paramount importance, among the other network nodes (Ojaghloo & Jannesary, 2015). The use of information from the message library is aimed at reaching routing optimization in completely new ways that might be useful for the rapid adjustment of the protocol through the reservation of data and hence the formation of the MANETs communication process (Pragadeswaran et al., 2024). This will be exemplified by the fact that the lexicon also includes some behaviors in message exchange, and these behaviors will be presented in terms of how the routing

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 1 (March), pp. 362-374. DOI: *10.58346/JOWUA.2025.I1.022*

*Corresponding author: Assistant Professor, Department of CS&E, VTU PG Centre Mysuru, Karnataka, India.

algorithms are integrated with the lexicon so as to devise a way for mobile hosts to reach their destinations through an adaptable choice of

the service route, not only over fixed paths but due to the adaptation of shortcuts in communication channels. 1. Elucidating on the topic of Lexicon in Message Exchange. The concept of a lexicon in message exchange refers to a report that is arranged in a certain order of message routing data in consequence of the fact that nodes get to the point where they can choose better and faster ways of transmitting the messages because of the information available to them (Lee & Teraoka, 2010). Through this heart, which improvers have voiced about this route, they? in turn, have encouraged their acquaintance with the routers and, i.e., led on a short, possible "quality operation." The use of the lexicon in routing is a radical yet promising method to make the networks smarter and more adaptable. The route whose main part has this characteristic is the one in which the message passes through a group of nodes that are closer to the destination and that change hosts after a certain time and become stations again in order for another set of nodes to pass the same route. Thereby, the networks will have a better chance to produce better results and defenses. Critical Points and Prospects The deployment of a lexicon of message exchange to the routing of the optimization in MANETs brings along both challenges and chances. The hard issues related to relevant network elements, e.g., the packet transmission link, the network natural dynamics, and the network security mechanisms, should be overcome in this way. Therefore, the issues of resource limitations, (Alo et al., 2018) network dynamics, and security considerations are primarily addressed Still, the idea of achieving a much more efficient and secure routing protocol by means of optimizing the lexicon presents an exciting path for doing some extra exploring and development.

2 Literature Survey

The Paper mobile ad hoc networks start at MANet's basic concepts and the applications they have been put into. The military's Tactical communication systems are the main application of the MANETs, and they also find commercial applications in interactive classes and business meetings (Dr. Rita Uzoma Alo, Nwokoro Ifeanyi Stanly 2018). The conversation takes a big look at networks with a base station to send signals, and the ones without stationary infrastructure that are usually mentioned as ad hoc networks (Haas, 2000) In this way, ad hoc networks are set up to transmit the data package from a node to another, which usually passes through several intermediate nodes before it reaches its final destination. All such attacks are meant for the decentralized scenario of MANETs and severely undermine secure communication. The article highlights the need for strong security solutions that are adapted to the specific limitations of MANETs, including bandwidth and power limitations (Savard, 2000). (Lee et al., 2002). Ad hoc networking is a fresh concept relating to the connection of mobile devices which are located wirelessly (Singha & Verma, 2019). It can be a disadvantage though, as it modifies the layout of the network topology. The nodes tend to shift from one geographical position (Moses et al., 2022) to another and hence, the topology is changing dynamically along with other aspects that were not expected. There is a variety of models for mobile platform (nodes) with particular movement that can be placed inside different transportation or hand-held devices that connect to the local network (Kawadia et al., 2003). The paper demands secure routing protocols to counter such attacks. The document proposes threshold cryptography as a solution to key management. The method divides the cryptographic key among multiple nodes, removing single points of failure and making the network attack-resistant. The periodic proactive renewal of secret shares also makes the network attack-resistant to long-term security (Sharma et al., 2021) breaches (Klos & Richard, 2005). The paper concludes by recognizing the vulnerability of MANET routing protocols to numerous attacks and

recommending holistic security solutions (Pirzada et al., 2014), such as encrypted routing messages and backup paths, to mitigate these threats. The paper, (Klos & Richard, 2005) in general, identifies the intricacy of MANET security and the need to incorporate sophisticated cryptographic methods and proactive security solutions to provide secure and reliable communication in dynamic, infrastructure-less network scenarios. The eavesdropping and analyzing of traffic is an example of passive security (Stajano, 1999) threats over mobile adhoc networks (MANETs) and flooding (Yi et al., 2006), black hole, wormhole, and spoofing attacks are classified as active security threats (Kang, 2020). There has been an observation in the literature regarding the need for perpetual advancement and integration of security measures within MANETs, so that its efficacy in different domains from military to civilian networking is not compromised. The article "Mobile (Omar et al., 2012) Ad-Hoc Networking with AODV A Review" describes the Ad-hoc On-Demand Distance Vector (AODV) routing protocol which is infamous in its applicability to Mobile Ad-Hoc Networks (Jhaveri, 2015). The authors outline the primary steps of the protocol that are based on the use of RREQ and RREP, and RERR messages for the dynamic route maintenance. In addition, the protocol's use of sequence numbers to eliminate routing loops and the delay in route adoption was pointed out as a mark of the protocol's ancestry within the DSDV family of protocols (Nuiaa et al., 2022). The paper also offers a very detailed explanation of wireless communications' attributes, including multi-hopping, where nodes transmit using limited radio power and require the assistance of other nodes to establish connections outside their ranges (Yi et al., 2005). It also refers to several of the challenges facing ad hoc networks, including having selfish nodes, poor ant behaviour, routing issues, and security concerns. In paper (Abusalah et al., 2008) Initially, offered general trends in wireless networks (Hu et al., 2006) and individual problems in ad hoc networks, (Aruna at al., 2023) but, of course, the whole paper is to be consulted in order to see the outlooks for this issue and to discover details in both areas.

The paper (Kannhavong, et al, 2007) begins by proposing the definition of MANETs, emphasizing the primary use in military tactical communication, and potential commercial uses and security issues related to worm whole attacks in the sensor networks (Tan et al., 2024). The article differentiates infrastructure networks that rely on a base station to convey information and infrastructure-less networks or ad hoc networks (Funabiki et al., 2006) in which the nodes talk to one another without infrastructure (Uushona & Penzhorn, 2005). For MANETs, the paper presents many security threats and solutions. The paper categorizes attacks as external and internal threats. External attacks are passive eavesdropping and active interference, for which encryption and confidentiality mechanisms are required. Internal attacks, normally by compromised nodes, require strong identification and rejection mechanisms. Janzadeh et al., (2009) Literature review on security risks in MANETs (Savard et al, 2000) is an extensive literature review of all risks and vulnerabilities pertaining to MANETs. Due to the lack of fixed infrastructure and the topology's dynamic nature in MANETs, they are highly susceptible to various forms of attacks due to open channels of communication and the absence of any central authority. Conventional security methods prove to be unsuitable because they are resource hungry. Hence, new methods like threshold cryptography and proactive key management are suggested. The paper approaches spread the cryptographic load over multiple nodes, which makes it less susceptible to a point of failure and increases the resilience of the network to internal and external attacks. In addition, the review examines several enhancements and variants of the AODV protocol to address particular issues, such as load balancing, route stability, and security attacks. The paper emphasizes the necessity of these variants to enhance the performance of the protocol in a broad spectrum of network conditions and environments. Despite the fact that the world has seen significant advancement in the past few years, the study still points to issues, such as energy efficiency and resilience to malicious attacks, that require

further research. (Klos & Richard, 2005) This comprehensive review is a valuable handbook to the development and current status of AODV in MANET applications.

Literature regarding trust models based on certification in mobile ad (Gupta & Pandey, 2014) hoc networks (MANETs) (Kambourakis, 2010; Omkar et al., 2012; Zhu et al., 2023) has mainly addressed secure communication and trust without relying on centralized infrastructure. The most widely used approaches, namely authoritarian and anarchic models, both provide different ways of handling public-key certificates and trust between nodes of a network. Authoritarian models have emphasized the focus of trust management by one or more certification authorities (CAs). They provide availability and scalability of services by distributing certification work among expert nodes through methods like threshold cryptography.Examples include the Zhou and Haas model (Sarumathi & Jayalakshmi, 2023) which has the focus on the coalition of servers for service availability, and the MOCA model, which has the focus on server selection with high physical protection and computing power (Balakrishna et al., 2010; Zhu &Boukerche, 2023).Conversely, anarchic models spread trust management over individual nodes, where each node is its own CA. This is highly certificate chain and node cooperation reliant for trust establishment, Models such as those of (Capkun et al., 2003) utilize proactive and reactive approaches, respectively, to manage trust relationships and certificate verifications. These models try to minimize certificate storage overhead and enhance verification efficiency, although they usually suffer from high communication overhead and certificate chain discovery complexity. Through a comprehensive taxonomy and performance analysis via stochastic Petri nets, this survey recognizes the strengths and weaknesses of different certification-based trust models, giving insights into their design and operational efficiencies.

According to the current study, lexicon network structure research offers a sophisticated explanation of the interactions amongst language features. Researchers can examine language as a network to study topics including phonetics, lexical processing, word acquisition, cognitive science, syntactic structures, and grammar learning. According to research studies using network science techniques, which are now an essential part of linguistics, word length, frequency, and semantic, phonetic, syntactic, and grammatical linkages all play a major part when establishing communities in phonological and syntactic networks(Bakshi & Sharma, 2013; Kumar & Srinivasan et al., 2022).The research also dwells to the framework of the mental lexicon, revealing that words are connected in a rich network by an abundant set of associative links. The mental lexicon has been structured according to syntactic and encyclopedic facts, as well as semantic and phonological levels, as demonstrated by word association databases, such as those based on Hungarian and Dutch. By demonstrating the co-occurrence and structure of various link types, community detection algorithms expose the depth and complexity of the mental lexicon's structural pattern. The approach provides useful insight into the functional and structural aspects of human language (Schiller et al., 2021).

Networks Behaviour Prediction for Mobile ADHOC

Several advanced techniques are utilized in prediction to mobile ad hoc networks (MANETs) with a view to improving prediction accuracy and dependability. These involve the use of machine learning techniques to learn from previous patterns and predict node behavior. Unsupervised learning is used here to group similar patterns of behavior and supervised learning to tag node behavior using training models over tagged data. In addition, supported by learning from the network environment, reinforcement learning is used to learn behavior prediction policies in an adaptive manner the use of trust-based models is an interesting feature of the methodology. By monitoring (Nguyen., 2008) past behavior of nodes and network activity, the models determine how trustworthy they are. Trust metrics

are calculated using factors, like rates of packet forwarding the time taken for responses and adherence, to protocol norms. Nodes that are deemed receive elevated levels of trustworthiness ratings and enable more accurate predictions of future behaviors, with increased certainty. In cases the trust-based system is employed to mimic the behavior of nodes and forecast potential anomalies or intrusions alongside statistical models and random processes, like Markov chains and Petri nets. Using a range of methods and strategies allows MANET systems to better anticipate behavior patterns and enhance network efficiency and security measures. When evaluating behavior prediction methods, in ad hoc networks (MANET) it is important to consider aspects such, as service accessibility, computational complexity, scalability and trust mechanisms. In this context we highlight the methods and effectiveness of two strategies, in forecasting behavior; anarchic models.

Authoritative Models; These models rely either centrally located or distributed certification authorities (CA).

(Zhou & Haas 1999) for instance employ a threshold cryptography method (denoted as k,n) in a distributed certification authority (CA) system wherein validation of a certification request requires the approval of k servers.

Raising the threshold k could lower the chances of collusion Might lead to needing servers, for certification and potentially impacting service availability. As a result, this strategy strikes a balance between security and service availability. In a similar vein, the MOCA model employs a fully distributed CA approach, which ensures high availability while increasing communication and processing complexity. These models are influenced by two parameters: server availability (λwhen) and interarrival time rates of authentication requests (\AReq); when one increases, the likelihood of successful certification (P{TS}) falls.

Anarchic Models: In contrast, anarchic models divide up trust management across all nodes and consider each one as a distinct CA. These models often employ either proactive or reactive certificate collection techniques. For instance, (Capkun et al., 2003) offer a public key management system where nodes collect and validate certificate chains as needed. Certification processes may be delayed by this resource-intensive system. The length of the certificate chain and the efficiency of the certificate collecting process are significant factors that affect overall service availability and computational load.

Ultimately, the decision between anarchic and authoritarian models is based on the particular needs of the mobile adhoc networks (MANET), including the demand for high service availability, resource limitations, and the required degree of security. While anarchic methods offer decentralized trust management with possible scaling advantages but more complexity in trust propagation and certificate management, authoritarian models offer reliable, scalable solutions with controllable overheads. Although anarchic approaches often have less scalability issues than authoritarian models since they do not rely on central repositories, they still have to deal with the difficulties of propagating trust and managing dynamic certificate chains.

A comparison of behaviour prediction methods in mobile ad hoc networks is shown in this table. Table 1 according to significant parameters:

Table 1: Mobile Ad hoc Networks (MANET'S) Significant Parameters

Trust Management	**Centralized or partially distributed certification authorities (CAs)**	**Distributed trust management across individual nodes**
Example Models	Zhou and Haas (1999), MOCA	Capkun et al. (2003)
Key Techniques	(k, n) threshold cryptography, fully distributed CA	Proactive/reactive certificate collection protocols
Service Availability	High, but depends on the number of required servers (threshold k)	Moderate to high, dependent on efficient certificate chain management
Scalability	High, centralization helps manage scalability issues	High, but complex due to dynamic certificate chain management
Computational Overhead	Moderate to high, due to cryptographic operations	High, due to on-demand certificate collection and verification
Security	High, robust against collusion with higher threshold k	High, but relies on trust propagation and the accuracy of certificates
Key Parameters	Inter arrival duration rates of authentication requests (λAReq), server availability (λAS)	Certificates chain length, efficiency of certificate collection protocol
Probability of Success (P{TS})	Decreases with increased λAReq and λAS	Dependent on efficient trust propagation and certificate management

3 Methodology

To assess and enhance the performance of MANETs with ANN and k-Nearest Neighbors (k-NN) classifiers, we may do the following:

Data Preparation

To prepare the data for performance analysis and MANET boosting using ANN and k-NN classifiers, we first collect or simulate a dataset containing relevant information such as node locations, signal intensities, and connection statuses. The data is then cleaned to remove any missing or erroneous values. The dataset is separated into training and testing sets, facilitates model evaluation. The characteristics are then standardized to ensure that they are on a same scale, which is crucial for many machine learning methods.

A function is created to automate the steps of cleaning the data, splitting it into training and testing sets, and standardizing the features. We train an ANN model and a k-NN classifier once the data is available. Binary cross-entropy loss and the Adam optimizer are used to generate the ANN model. It is composed of a sigmoid output layer and layers with relu activations. Five neighbours are used by default to train the k-NN classifier. Both models are evaluated using metrics such as F1-score, accuracy, precision and recall,

Grid search is used to determine the ideal number of neighbours to adjust hyper parameters and improve performance, particularly for the k-NN classifier. To further enhance performance, the predictions from the enhanced k-NN and ANN models are then included into a voting classifier. By using ensemble approaches and tuning, this methodical procedure guarantees optimal performance and well-prepared data for the models' training.

4 Ad hoc Network Data Lexicon

Sample of network data and Ad hoc network data lexicon with its data types and size are shown in Table 2.

Table 2 : Sample of Network Data and Ad Hoc Network Data Lexicon

SL No.	Term	Description	Data Type	Size (Bytes)
1	Packet	A unit of data transmitted in a network, consists of both header information (e.g., source and destination addresses) and payload (actual data).	Structure	Variable
2	Control Message	A type of packet used for network management purposes, such as route discovery, route maintenance, and synchronization.	Structure	Variable
3	Beacon	A type of control message periodically broadcasted by nodes to advertise their presence and network-related information.	Structure	Variable
4	Routing Table Entry	A data structure maintained by each node containing information about known routes to other nodes in the network.	Structure	Variable
5	Neighbor Table Entry	A data structure maintained by each node containing information about neighboring nodes within communication range.	Structure	Variable
6	Link State Information	Information about the state and characteristics of links between nodes in the network, used for routing decisions.	Structure	Variable
7	Route Request Packet	A packet sent by a node to request a route to a destination node from the network.	Structure	Variable

Feature Engineering

To enhance model performance in MANETs, the development of features for ANN and k-NN classifiers comprises several crucial tasks. The first stage in dealing with missing or wrong numbers is data cleansing. Choose pertinent attributes including connection statuses, signal intensities, and node locations. To capture other patterns, such as average signal intensity or distance measurements between nodes, create new features based on already present ones. To establish a consistent scale, which is essential for both ANN and k-NN, modify features via normalization or standardization.PCA is one dimensionality reduction approach that may be used to decrease features and improve the speed of computing. Divide the data into training and testing sets so that the model's performance can be reliably measured. The fact that some of the options that were used to supply the columns should finally run in scale with Regular Scaler or Min Max Scaler is crucial. For the purpose of training ANN and k-NN classifiers in MANETs, the effective feature engineering approach assures that the data is effectively increased.

Model Training

To enhance performance in MANETs, ANN and k-NN classifiers must go through many essential phases of model training. To capture multiple complex patterns, build a multi-layered ANN with a sigmoid activation function in the output layer and ReLU for the hidden layers and use the Adam optimizer and binary cross-entropy loss function to create the ANN. Train the model on the standardized training set while measuring development in performance using accuracy metrics. To identify the

optimal number of neighbors for the k-NN decoder, conduct a grid search with cross-validation on the standardized training set to construct the k-NN model. Evaluate the two models on the test set using classification metrics like F1-score, precision, and recall. Improve model parameter tuning through cross-validation and hyper parameter optimization, or integrate boosting methods such as fused ANN and k-NN predictions to improve performance: optimization is shown in Fig. 1 by an optimal route between increased routing and security.

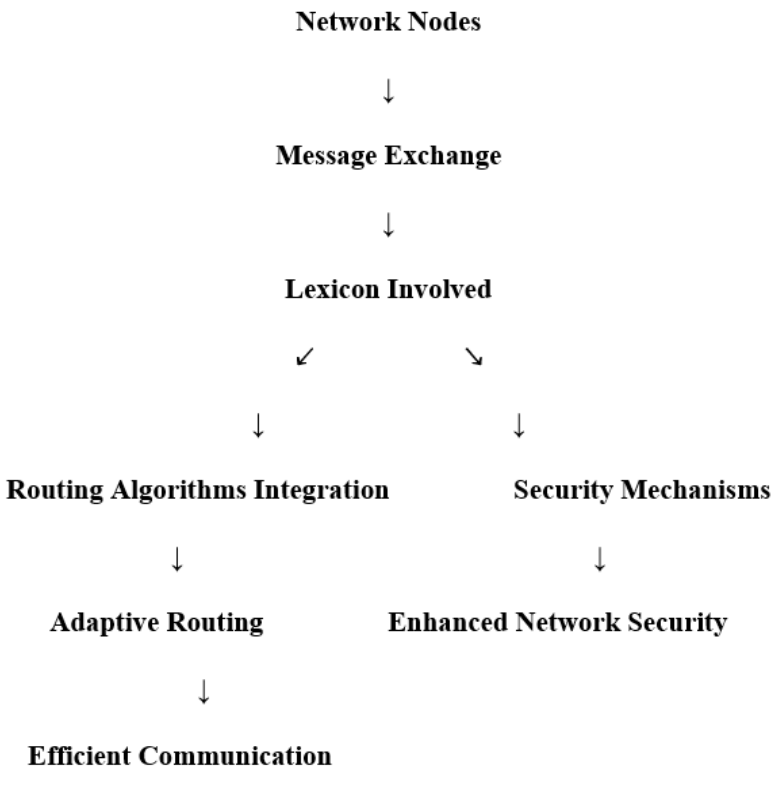

Figure 1: Shows the Impact of Lexicon on Routing Optimization

5 Performance Analysis

Performance analysis examines the performance of ANN and k-NN classifiers using a variety of factors. Use consistent data to train the models. Then, measure performance using the test set. F1-score, recall, accuracy, and precision are important metrics that give an exhaustive analysis of each model's strengths and weaknesses. During ANN training, keep an eye on accuracy and loss to determine over fitting or under fitting. To further understand classification errors, we use confusion matrices to assess the true positive, false positive, true negative and false negative rates. Ensemble models are required because MANets are evolving; therefore, it's challenging to build a static model.

After comparing the results across models to determine which one performs better in various situations, this strategy uses techniques like cross-validation, hyperparameter tuning, and ensemble methods, including merging ANN and k-NN predictions, to further boost performance. You may find challenges regions and put measures in motion to improve the classifiers' overall accuracy in MANETs by thoroughly reviewing and comparing these metrics.

Boosting Performance

Applying a variety of complex techniques is necessary to improve the performance of ANN and k-NN classifiers. In order to maximize parameters like learning rate, batch size, and the number of hidden layers and neurons, hyper parameter tuning for the ANN may be accomplished by methods like grid search or random search. Regularization techniques like dropout can help reduce over fitting.

To avoid different dangers, the number of neighbours using the k-NN classifier should be adjusted by cross-validation. Feature selection and engineering can significantly enhance the model's performance by removing superfluous or redundant elements and creating new, useful ones. By combining the benefits of ANN and k-NN, ensemble techniques like voting classifiers and stacking can improve forecast accuracy.

To improve the model's performance and resilience even more, strategies like bagging and boosting might be applied. To be confident that the improvements are indeed resulting in better MANET performance, it is imperative to regularly evaluate the model’s using metrics like accuracy, recall, and F1-score is shown in Fig 2.

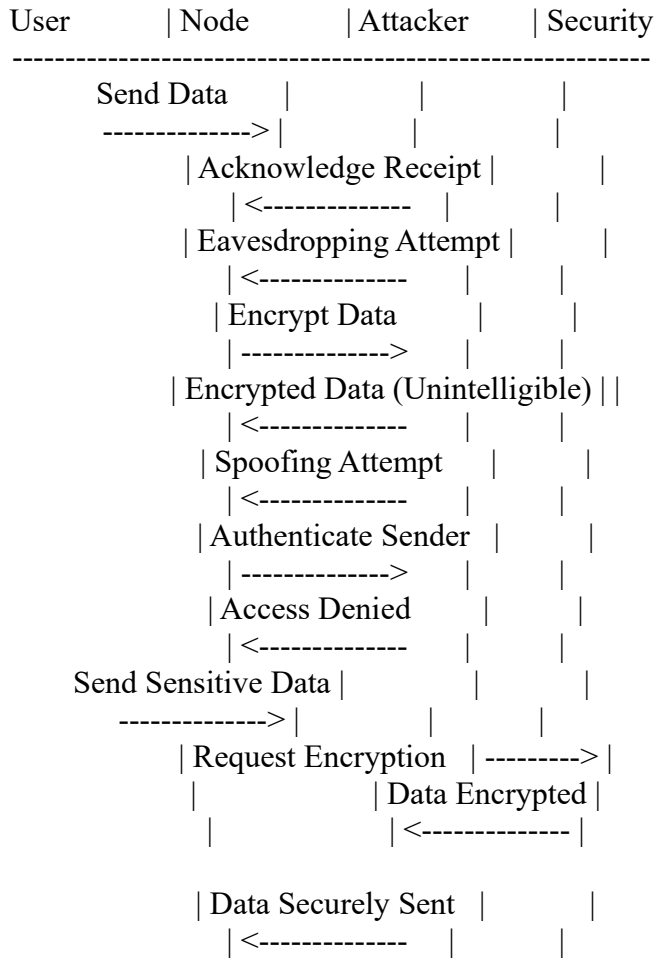

Figure 2: Security Threats and Solutions in MANETs

6 Conclusion

Briefly put up, studies investigating lexicon in mobile ad hoc networks (MANETs) has shown how important it is for improving communication, security, and routing in these dynamic, infrastructure-less circumstances. Through a method of arranging data, in the lexicon system helps in facilitating smoother communication and leads to reduced network congestion while boosting overall efficiency. Based on research findings it has been suggested that incorporating Lexicon technology could lead to improved routing protocols with Quality of Experience (QoE) and Quality of Service (QoS) along, with heightened security measures. The article highlights the importance of addressing challenges such, as resources, unpredictable movement patterns and security vulnerabilities, in MANET networks. To better predict and manage network functions effectively different ideas and methods have been proposed, including machine learning algorithms and trust-based networks. When looking at authoritarian behavior prediction models side by side—the focus is, on the balance, between decentralized and hierarchical trust management—each comes with its advantages and obstacles to navigate. In terms and upon reflection, on the matter at hand suggests that exploring assessment in MANET environments holds promise, for further study and advancement. MANETs will become less susceptible and effective as a result of improvements in behavior prediction algorithms, security measures, and routing protocols. To satisfy the changing needs of mobile ad hoc networks, continual lexicon-driven approach optimization and integration will be required as technology develops.

ACKNOWLEDGEMENTS

Funding Details

This research received no external funding.

Authors' Contributions

All authors contributed toward data analysis, drafting and revising the paper and agreed to be responsible for all the aspects of this work.

Declaration of Conflicts of Interests

Authors declare that they have no conflict of interest.

Use of Artificial Intelligence

Not applicable

Declarations

Authors declare that all works are original and this manuscript has not been published in any other journal.

References

[1] Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys & Tutorials, 10*(4), 78-93.

[2] Alo, R. U., Stanly, N. I., & Onwe, N. F. (2018). Mobile Ad Hoc Network (MANET): Applications, Benefits and Performance Issues in a Global Positioning System. *International Research Journal of Engineering and Technology (IRJET), 5*(11), 983-987. https://www.irjet.net/archives/V5/i11/IRJET-V5I11188

[3] Aruna, O., Sameerunnisa, SK & Vedantham, R. (2023). Routing in Mobile ad Hoc Networks Using Machine Learning Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(4), pp. 84-95. https://jowua.com/wp-content/uploads/2023/12/2023.I4.006.pdf

[4] Bakshi, A., Sharma, A. K., & Mishra, A. (2013). Significance of mobile AD-HOC networks (MANETS). *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2*(4), 1-5.

[5] Balakrishna, R., Rao, U. R., Ramachandra, G. A., & Bhagyashekar, M. S. (2010). Trust-based Routing Security in MANETS. *International Journal of Computer Science and Information Technolgy, 4*(3), 547-553. https://doi.org/10.1007/978-3-642-36169-2_3

[6] Funabiki, S., Isohara, T., Kitada, Y., Takemori, K., & Sasase, I. (2006, December). Public key management scheme with certificate management node for wireless ad hoc networks. In *Proceedings of the international multiconference on computer science and information technology.*

[7] Gupta, R., & Pandey, R. (2014). A survey of routing optimization techniques in mobile ad hoc networks. *Journal of Network and Computer Applications, 40*, 211-224.

[8] Haas, Z. J. (2000). A new routing protocol for the reconfigurable wireless networks. *Retrieved from* http://www.ee.cornell.edu/~jaas/wnl.html

[9] Hu, Y-C., Perrig, A., & Johnson, D. (2006). Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 370-380.

[10] Janzadeh, H., Fayazbakhsh, K., Dehghan, M., & Fallah, M-S. (2009). A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. *Future Generation Computer Systems, 25*(8), 926–934.

[11] Jhaveri, R. (2015). Mobile ad-hoc networking with AODV: A review. *International Journal of Next-Generation Computing, 6*, 165-191.

[12] Kambourakis, G., Konstantinou, E., Douma, A., Anagnostopoulos, M., & Fotiadis, G. (2010). Efficient certification path discovery for MANET. *EURASIP Journal on Wireless Communications and Networking, 2010*, 1-16.

[13] Kang, M. (2020). The Study on the Effect of the Internet and Mobile-Cellular on Trade in Services: Using the Modified Gravity Model. *Journal of Internet Services and Information Security, 10*(4), 90-100

[14] Kannhavong, B., Nakayama, H., Nemoto, Y., & Kato, N. (2007). A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications, 14*(5), 85-91.

[15] Kawadia, V., Zhang, Y., & Gupta, B. (2003, May). System services for ad-hoc routing: Architecture, implementation and experiences. In *Proceedings of the 1st international conference on Mobile systems, applications and services* (99-112).

[16] Klos, L., & Richard, G. G. (2005). Reliable ad hoc group communication using local neighborhoods. In *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.* (3), 361-368. IEEE.

[17] Kumar, S., & Srinivasan, P. (2022). Mobile ad-hoc network. *International Journal of Applied Engineering Research, 9*, 9711-9715.

[18] Lee, J. H., & Teraoka, F. (2010). Guest editorial: Advances in wireless mobile and sensor technologies. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable* Applications, 1(2/3), 1-2.

[19] Lee, S., Han, B., & Shin, M. (2002). Robust routing in wireless ad hoc networks. In *Proceedings. International Conference on Parallel Processing Workshop* (73-78). IEEE.

[20] Moses, M. B., Nithya, S. E. & Parameswari, M. (2022). Internet of Things and Geographical Information System based Monitoring and Mapping of Real Time Water Quality System. *International Journal of Environmental Sciences, 8*(1), 27-36. https://www.theaspd.com/resources/3.%20Water%20Quality%20Monitoring%20Paper.pdf

[21] Nguyen, D., Zhao, L., Uisawang, P., & Platt, J. (2008). Security routing analysis for mobile ad hoc networks.

[22] Nuiaa, R. R., Alsaeedi, A. H., Alkafagi, S. S., & Alfoudi, A. S. D. (2022). A Critical Review of Optimization MANET Routing Protocols. *Wasit Journal of Computer and Mathematics Science, 1*(4). https://doi.org/10.31185/wjcm.94

[23] Ojaghloo, M., & Jannesary, A. (2015). Investigate all attacks on Mobile Wireless Networks and Finding security solutions. *International Academic Journal of Innovative Research, 2*(2), 17–27.

[24] Omar, M., Challal, Y. & Bouabdallah, A. (2012). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *Journal of Network and Computer Applications, 35*(1), 268-286. https://doi.org/10.1016/j.jnca.2011.08.008.

[25] Pirzada, S., Portmann, M., & Colman-Meixner, C. (2014). Trust-based security in MANETs. *Ad Hoc & Sensor Wireless Networks, 20*(3-4), 201-223.

[26] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., Aakash, R., & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme Using Homomorphic Encryption. *Archives for Technical Sciences, 2*(31), 148–158. https://doi.org/10.70102/afts.2024.1631.148

[27] Sarumathi, R., & Jayalakshmi, V. (2023, February). A Novel Trust Value Based Mobile Ad hoc Networks (MANETs) Security. *In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC)* (933-939). IEEE. https://doi.org/10.1109/ICCMC56507.2023.10084006

[28] Savard, J. (2000). One-way hash functions. A Cryptographic Compendium. Retrieved from http://fn2.freenet.edmonton.ab.ca/~jsavard/mi0605.htm

[29] Schiller, N. O. (2021). The mental lexicon. Oxford University Press. DOI: 10.1093/OBO/9780199772810-0282

[30] Sharma, S., Kumar, K., & Kashyap, S. (2021). Security issues and challenges in MANET: A review. *Egyptian Informatics Journal, 22*(3), 1-9.

[31] Singha, S. C., & Verma, M. K. (2019). Integration of AIDC Technology in Mobile via QR Code for Enhancing the Library Services: A Case Study of Don Bosco College Central Library, Arunachal Pradesh. *Indian Journal of Information Sources and Services, 9*(2), 44–48. https://doi.org/10.51983/ijiss.2019.9.2.626

[32] Stajano, F. (1999, April). The resurrecting duckling. In *International workshop on security protocols* (183-194). Berlin, Heidelberg: Springer Berlin Heidelberg.

[33] Tan, W., Sarmiento, J., & Rosales, C. A. (2024). Exploring the Performance Impact of Neural Network Optimization on Energy Analysis of Biosensor. *Natural and Engineering Sciences, 9*(2), 164-183. https://doi.org/10.28978/nesciences.1569280

[34] Uushona, N., & Penzhorn, W. T. (2005, June). Towards the Security of Routing in Ad Hoc Networks. In Proceedings of the IEEE International Symposium on Industrial Electronics, 2005. *ISIE 2005. 4*, (1783-1788). IEEE. https://doi.org/10.1109/ISIE.2005.1529203

[35] Yi, P., Dai, Z., Zhang, S., & Zhong, Y. (2005). A new routing attack in mobile ad hoc networks. *International Journal of Information Technology, 11*(2), 83-94.

[36] Yi, P., fei Hou, Y., Zhong, Y., Zhang, S., & Dai, Z. (2006). Flooding attack and defence in ad hoc networks. *Journal of Systems Engineering and Electronics, 17*(2), 410-416

Authors Biography

T. Yogesha has obtained M.Tech specialized in software engineering from VTU Belagavi and currently pursuing PhD in Dept of CSE VTU Mysuru. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, VTU, PG Center Mysuru. He is actively involved in various research activities and has published research papers in reputed national and international journals

Dr.S.N. Thimmaraju completed his PhD from VTU, Belagavi and is currently working as Professor & Program Coordinator in VTU PG Centre, Mysuru. Previously he has worked as Regional Director in VTU Regional Centre, Mysuru. His area of interest is Graph Theory and Computer Networks. He has teaching experience of 22 years and has published several Research Papers in National & International Journals and has guided 3 PhD students in VTU, Belagavi. He is the member of Board of Studies, Board of Examination for VTU and other Universities.