Iraqi Journal for Computer S cience and Mathematics
Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM e-ISSN: 2788-7421 p-ISSN: 2958-0544

Integrating Intelligent Systems in MANET- IoT Environment based on Subjective Context

Abdulbasit ALAZZAWI[1], Qahtan M.Yas[2]*

[1]Diyala University, College of Science, Diyala, IRAQ,

[2]Diyala University, College of Veterinary Medicine, Diyala, IRAQ,

*Corresponding Author: Qahtan M.Yas

DOI: https://doi.org/10.52866/ijcsm.2024.05.02.003
Received October 2023; Accepted Janeuary 2024; Available online March 2024

ABSTRACT: The Internet of Things (IoT) has cultivated a promising environment, pivotal across diverse sectors via MANET protocols within the w.w.w. This technology significantly contributes to advanced services for mobile devices in the MANET-IoT domain. However, MANET encounters security challenges, notably malicious attacks as a prime concern. To counter these threats, preventive measures like subjective-context evaluation and node protection are employed, ensuring data packet integrity before delivery. This study aims to enhance the performance of a novel reactive protocol, integrated with a fuzzy system within the MANET-IoT environment. The methodology is implemented in two directions: 1) Establishing a secure network founded on trust parameters and shortest path selection. 2) Incorporating an integrated fuzzy system into an improved reactive routing protocol within the MANET environment. Subjective context ensures a secure milieu, evaluating nodes before packet delivery based on trust and shortest path. The fuzzy system's rules determine the network's probability distribution, contingent upon trust and the number of hop counts. The proposed routing protocol is evaluated both pre- and postattacks during packet transmission. Results demonstrate its superiority in packet transmission over the original protocol. Three scenarios evaluate packet delivery fraction (PDF), end-to-end delay (E2E), and normalized routing load (NRL). FS-AODV's percentages were 0.9873% against AODV's 1.9871% without drop) and 0.8419% with a drop for PDF. FS-AODV's percentages stood at 0.0006% against AODV's 0.0007% without a drop and 0.0005% with a drop for E2E. In contrast, FS-AODV's percentage was 0.058%, AODV at 0.0127% without a drop, and 0.066% with a drop for NRL.

Keywords: MANET, Internet of Things, Fuzzy System, Subjective Context, Trust Factor, Shortest path factor, malicious attacks

1. INTRODUCTION

The IoT environment encompasses a spectrum of diverse devices and sensors that facilitate versatile intercommunication and the transmission of vast data volumes [1] [2]. Within the supreme priorities, the protection of personal data can be highlighted as the goal that strives to build trust in the exchange of personal information. There are several approaches that can be put in place to enhance the privacy such as; Authentication, Encryption, and limited access. Of these, the trust factor along with the optimal routing has an important role to play as a part of privacy enhancement as one of the measures of access control. Therefore, the combination of the trust factor and the optimal routing reduces the inter-device communication and adds extra protection against malicious attacks [3] [4]. Thus, the combination of the trust factor and the shortest path in the complex structure of IoT can be considered to play the part of a backbone in ensuring secure communication between devices. Unlike the hosts in the conventional Internet, IoT devices have unique characteristics, which require a dynamic assessment that considers the ability to join and leave the network and depending on the trust factor and the selection of the best path [3]. In the field of artificial intelligence, various methods have advanced the improvement of reactive protocols in the context of MANET-IoT. Among these methodologies, the application of fuzzy systems stands out as a cornerstone, showcasing its efficacy in numerous research endeavors and offering robust solutions [5].

26 *Corresponding author: author@organization.edu.co
http://journal.esj.edu.iq/index.php/IJCM

In the present study, we amalgamate the capabilities of a fuzzy system with a reactive protocol, the amalgamation guided by fuzzy rules that dictate the selection of the optimal route in terms of both shortest path and trust quotient. Consequently, this symbiotic routing protocol mechanism is calibrated on the bedrock of trust levels and minimal hops, thereby engendering a secure conduit that ensures successful packet transmission to the designated destination [6][7]. The paper's structure unfolds as follows: Section 2 delves into pertinent literature, elucidating the landscape of relevant studies. In Section 3, we introduce the novel routing protocol, conceived in congruence with trust levels and optimal paths. Section 4 scrutinizes the empirical findings garnered. Finally, Section 5 encapsulates the essence of the study through its concluding remarks.

1.1 CONTRIBUTION OF STUDY

The essence of this study is to propose an effective routing strategy best suited for the complexity of MANET-IoT. The main objective is to introduce a higher level of protection to the routing processes so that data packets are transmitted as efficiently as possible. This effort was followed by the integration of a fuzzy system with the AODV protocol, which heralded a reactive regime based on trust levels and the best possible routing paths to achieve protected routing nodes.

The importance of this integration rises sharply within the framework of MANET-IoT, where the path from source node to destination or gateway is winding and passes through a number of routing nodes which are formed spontaneously. In essence, the primary contributions of this study coalesce as follows:In essence, the primary contributions of this study coalesce as follows:

- Design of a strong routing protocol in the MANET-IoT domain to address secure data packet transmission to enhance the security of the network.
- The enhancement of a reactive routing protocol coupled with a fuzzy system in AODV based on trust levels and optimum path for enhancing the security of the routing nodes in MANET-IoT environment.
- Routing nodes' distribution during route discovery based on the subjective context mechanism for route assessment in the MANET-IoT.
- Evaluation of this mechanism, based on minimum hop count and trust levels before the packet transmission process to check trust during delivery.
- Assurance of route node credibility, pivotal in effecting secure and robust packet delivery.

1.2 SUBJECTIVE CONTEXT

Subjective context comprises of trust model that originates from the perception of the researchers, as defined by the term 'opinion' which means individual outlook [8]. The subsequent modeling of trust between nodes was based on this principle of opinion. Typically, nodes in a MANET environment are many and are distributed over a large geographical area. However, while moving along the paths, a node may not be fully certain about the trust level of the neighboring nodes because of the lack of sufficient information. This subjective paradigm involved a host of things, including the general ideas such as dichotomy and odds, and others that relied on belief theory. Special emphasis should be made to the way the discount factor can help determine trust levels. Hence, the discount factor emerges as a critical factor that defines the development of trust along the route [9]. Therefore, the subjective context provides an opportunity for creating a mapping that corresponds to the trust factor in accordance with the opinion principle.

1.3 TRUST MODEL

The trust model assumes the highest importance in analyzing and designing secure distributed systems in the context of MANET [10]. In a similar vein, the trust factor arises as the key enabler of the implementation of the concept of decision-making within the framework of this study [11]. The determination of the trust level depends on the relationship that each node has with the other nodes in the network.

Ad hoc networking is based on the trust model that includes direct and recommended, or indirect, trust assessments [1]. With regard to open networks, the process of authentication implies that nodes base their decisions on the recommendations of other nodes in the network, to determine trustworthy paths. Thus, nodes which gained trust perform the function of authentication servers within ad-hoc networks (AS). The ensuing exposition delves into an elaborate discussion of the trust model:The ensuing exposition delves into an elaborate discussion of the trust model:

(i) In other words, the direct trust factor refers to the level of trust that node 1 has on the neighboring node, depending on the experiences that node 1 has had with the said neighboring node. As a result, the direct trust relationship signifies node 1's capacity to assess the trust level of neighboring node 2 when embarking on route discovery.

(ii) The indirect trust factor leverages a recommendation mechanism between nodes within a shared route. This indirect trust dynamic operates through node 1's endorsement extended to node 3, while the trust dynamic between node 2 and node 3 remains a direct trust interaction. This orchestration culminates in the establishment of an indirect trust connection between node 1 and node 3.

2 RELATED WORKS

Waleed Alnumay et al. [12] introduced a novel quantitative trust model for MANET-IoT, merging direct and indirect trust models to compute a comprehensive trust value for nodes.Gautam M and A. R. Mahajan [13] harnessed the secure neighborhood trust verification protocol to devise a network-based multipath routing approach upon the discovery of secure routes. This method combined the Dolphin Echolocation algorithm for optimal connectivity within MANET.HUAQIANG XU et al. [14] proposed a trust-based broadcast (TPB) system to thwart malicious node attacks, achieving trust levels and reducing overhead. Their lightweight trust model employed both direct and indirect trust principles for trust level calculation.M. Bharti et al. [15] presented a secure routing scheme ensuring route safety and minimal energy consumption via two algorithms. The first determines optimal cluster heads, while the second calculates trust values and energy-efficient paths for secure connections.A. Beghriche and A. Bilami [16] introduced a novel blend of trust, fuzzy theory, and gray theory in MANET, aiming to establish trust levels among neighboring nodes. This approach facilitates routing decision-making by establishing trust relationships among network nodes.P.K. Bai [17] proposed the Routing Manager-Based Safe Rate Analysis System (RMBSRA) to enhance multicast routing using bandwidth computation and network traffic identification. Real-time analysis of secure routes via RMBSRA demonstrated enhanced performance compared to existing systems.Yamini, K. Anish Pon et al. [18] presented the ITrust mechanism, leveraging the ETERE scheme to probabilistically detect misbehaving nodes and secure MANET routing. This mechanism employs a reliable routing table for periodic evaluation of node behavior, effectively preventing intrusions.V. Thirunavukkarasu et al. [19] introduced ACEPTR, a Clustering-based and Angular-based Energy Proficient Trusted Routing Protocol. This approach calculates Node Credit Score (NCS) and leverages the angular energy mechanism to significantly reduce energy consumption, outperforming traditional schemes.
Pushpender Sarao [20] devised an enhanced Fuzzy-based Energy Efficient AODV (FEEAODV) routing approach for ad-hoc wireless networks. This method demonstrated improved network lifetime and routing cost compared to conventional AODV.G. Yu, C. Xia, and J. Chen [21] crafted a lightweight fuzzy collaborative evaluation model (LFCTEM) for edge devices, calculating confidence ratios based on fuzzy parameters. The approach mitigated selfish behavior and enhanced cooperation, thereby improving the CEEC network's interference and reliability.

3 MATERIAL AND METHODS

3.1 PROPOSED DESIGN

Artificial intelligence (AI) technologies have emerged as pivotal problem-solving tools within the complex domain of MANET-IoT. The incorporation of the fuzzy system stands out as a potent solution to mitigate challenges endemic to this wireless network paradigm. This integration involves entwining the fuzzy system with a reactive routing protocol entrenched within the MANET fabric [22].In MANET, the bedrock of the trust relationship springs from direct node interactions, delineated as either trust relationships or potential trust relationships. These evaluations hinge on node recommendations, culminating in the delineation of trustworthy paths. Notably, a fuzzy system is embraced within the MANET-IoT landscape, adopting a direct trust model. This augmented model enriches the trust relationship mechanism, seamlessly oscillating between direct and indirect recommendation trust models, thereby engendering the collection and computation of trust values between nodes and assessing hops through fuzzy system rules [20].These rules of the fuzzy system pivot around input values denoted by parameters such as node trust levels and optimal path selection during data packet transmission. To substantiate the efficacy of these methodologies, a simulation tool is deployed to juxtapose and appraise three protocols: FS-AODV, AODV with and without packet drops. The culmination of this analysis furnishes definitive insights. Refer to Figure 1 for a visual depiction of the MANET-IoT environment's procedural model.

.

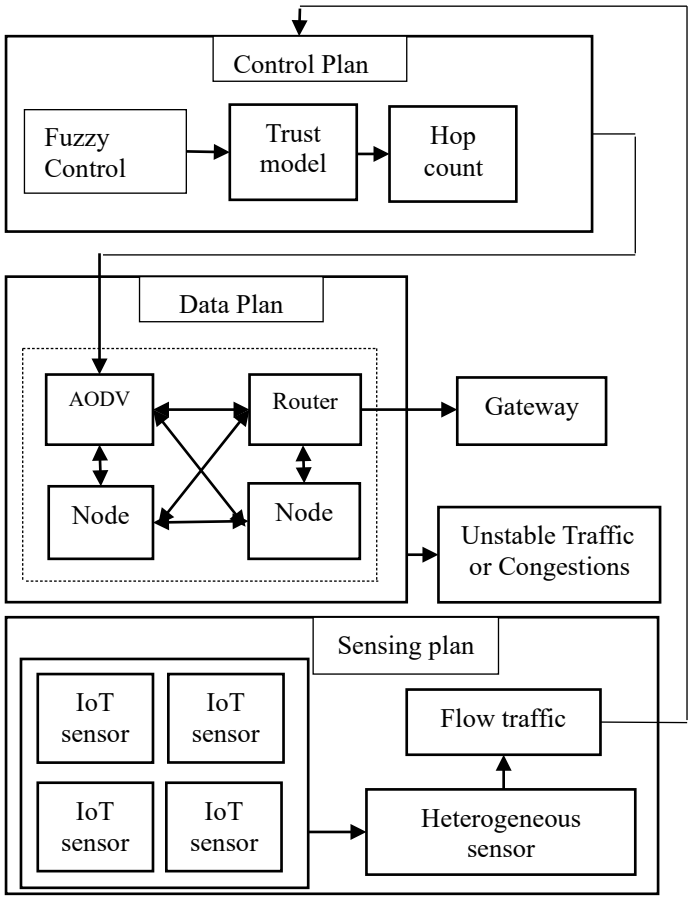

FIGURE 1. MANET-IoT Environment Procedure

Within this environment, the trust mechanism operates through two pivotal paradigms: The two types of trust are direct trust, and indirect trust. The direct trust relationship is derived from the assessment of nodes along the path and includes such features as routed packet nature, dropped packet frequency, and routing packet error rates. In its simplest form, the direct trust between node 1 and node 2 is the process of determining the trust level with information that measures the mutual dependence between the two nodes. This evaluation results in the determination of trust level, which is in essence the trust that both node 1 and node 2 have for each other.

3.2 FUZZY SYSTEM IMPLEMENTATION

In this segment, the fuzzy system, which is a powerful tool of artificial intelligence, works hand in hand with the reactive protocols in the context of the MANET environment [23]. This technique carves its own market when dealing with data expressed in mathematical forms, effectively solving complex problems containing ambiguous characteristics. In the light of this study, fuzzy parameters are applied which include the trust level and the hop count which is useful in determining the best path. The design outlined here coordinates a juxtaposition of these two variables, both vital in the context of the MANET domain. For a graphical representation of the following description, the reader is advised to turn to figure 2 where the block diagram represents the control components inherent in the fuzzy system.

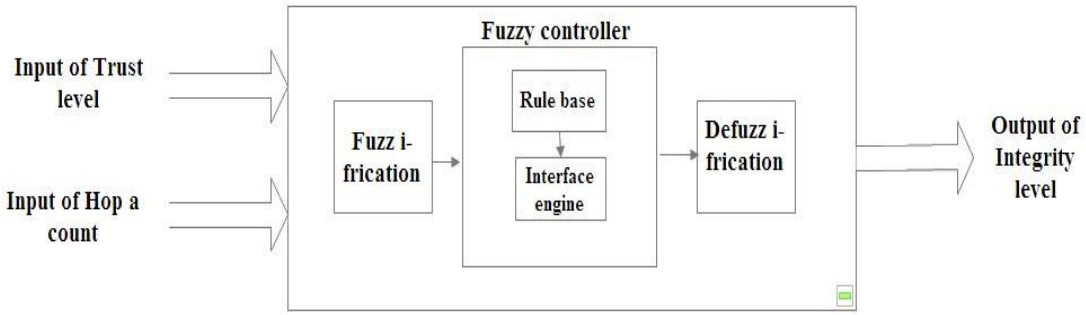

FIGURE 2. Control of the Fuzzy System

The fuzzy system is therefore presented as a friendly tool, capable of drawing out definite conclusions based on the probabilistic nature of the data used. In this regard, the fuzzy system emerges into the foreground, which is charged with the mission of computing the best trajectory. This technique follows the "if-then" rule of operation in order to compute variable values to determine the best route. In other words, this system works in a way that assesses variable values, choosing the highest trust level combined with the minimum hop count, ending in the selection of the shortest path. Thus, the integration of this fuzzy system with reactive protocol results in satisfactory results that enhance the AODV protocol performance. Please, see Figure 1 for the visual representation of the fuzzy rule regarding the calculation of the parameter value.

TABLE 1. Rules of Fuzzy System

Input variable (T)	**Input variable (HC)**	**Output variable (IL)**
Low	Short	Normal
Low	Medium	Few
Low	Long	Poor
Moderate	Short	Good
Moderate	Medium	Normal
Moderate	Long	Few
High	Short	V. Good
High	Medium	Good
High	Long	Normal

In this section, a detailed analysis of the expected benefits arising from integration of fuzzy logic and the AODV routing protocol is made. The incorporation of an intelligent system in the context of MANETs can be considered as a significant advancement towards addressing the difficulties and risks associated with protecting routing protocols in the vast domain of MANET-IoT. This synergy that forms the foundation of this study coherently integrates some of the most complex principles originating from the field of intelligent systems with the ever-fluid environment of MANETs to deliver a polished and secure routing protocol. Realizing the benefits of integrating fuzzy logic with the routing protocol mandates the fulfillment of certain prerequisites:Realizing the benefits of integrating fuzzy logic with the routing protocol mandates the fulfillment of certain prerequisites:

- Integrating Fuzzy Logic with AODV Protocol:

The integration process is focused around the combination of an intelligent system based on fuzzy logic and the AODV routing protocol. This fusion can be regarded as a promising way to enrich the process of routing with increased flexibility and contextual awareness. Fuzzy logic stands out in handling ambiguous and imprecise data in a balanced manner, and this cooperation is well complemented by the flexibility of AODV, which forms a solid synergy that addresses the complexity of MANETs' inherent dynamism.

- Enhancing Trust-Based Routing:

The most important application of intelligence in the system can be well explained through the establishment of trust-based routing protocols. This system is full of trust levels which scrutinizes the nodes in the network hence ensuring secure transfer of data. The intelligent system on-line in the perpetual dynamic mode prepares the routing choice based on the trust feedback in real-time; thus, an inherently adaptive mechanism is integrated to adapt to the typical fluctuating changes inherent in the MANET topology as part of the inherent nature of MANETs.

- Securing Routing Nodes:

Another pivotal facet of this integration lies in bolstering the security of routing nodes. Here, the intelligent system assumes a pivotal role by evaluating not just trustworthiness but also optimizing routes in consideration of the shortest path. This dual assessment guarantees that data packets navigate a trajectory that mitigates potential vulnerabilities

while concurrently expediting their conveyance. This proactive intelligence constitutes a tangible augmentation to the overarching security fabric of the routing protocol.

- Contextualized Evaluation:

In the context of the MANET environment, which is defined as the environment where nodes are self-organized and routes are constantly changing, the intelligent system introduces the factor of contextual evaluation into play. This implies that before the actual data is transmitted, the system checks the reliability of the nodes based on their location and functionality in the network. It is thus evident that by the use of parameters like minimal hops and trust levels, the system is able to select each of the route nodes in such a way that they fully satisfy the security specifications of the particular protocol being used.

As a result, the integration of the intelligent system into the MANET milieu goes beyond the concept of routing protocol. As the intelligent systems' principles can be applied to the development of the new, self-organizing, and context-aware routing protocol. This synergy results in a significant input in the protection of the flow of data packets in the network and effectively managing the unique features of the MANET-IoT environment. This new routing protocol hence enhances the security and reliability of data packet transmission through the dynamic and uncertain nature of network environments.

4 RESULTS & DISSOCIATION

This section delves into the outcomes gleaned from the parameters embraced in this study. A network topology is charted based on precise metrics, emblematic of the routing protocol's functionality within the MANET-IoT milieu. The simulation methodology is employed, encompassing three key metrics: the total count of nodes in the network, the maximum velocity, and the pause interval, all encapsulated in Table 2

TABLE 2. Simulation Parameters

Parameter	Value
Routing Protocol	Ad hoc on-demand distance vector protocol
Transport Protocol	UDP
Map Size	750m X 750m
Mobility Model	Random waypoint
Packet Size	512 bytes
Traffic Type	CBR
Total nodes	10 IoT source nodes and 80 MANET nodes
Malicious nodes	5 MANET nodes
Simulation time	900s
Pause times	10, 20,40,60,80,100,120,140
Sensor node mobility	10 m/s

The evaluation of results encompassing three distinct performance metrics transpires through the utilization of the NS-2 simulator, unfolding across three distinctive scenarios. These results afford a comprehensive comparative analysis of the performance of the newly introduced FS-AODV protocol against the backdrop of the AODV routing protocol, both in the presence and absence of dropped packets. Employing the NS-2 simulation environment, this study meticulously computes three pivotal parameters, accounting for the original AODV protocol as well as its enhanced variant.

The outcomes, succinctly depicted through diverse graphical representations, serve to underscore the efficacy of this approach. Delving deeper, the results unfurl a comprehensive portrayal of varied scenarios enacted within the MANET-IoT ecosystem, embodying a meticulous and detailed assessment of the intricate dynamics inherent to this environment.

4.3 PERFORMANCE MEASURES

Within this section, the crux lies in the computation of three fundamental benchmarks pivotal for assessing the efficacy of MANET protocols. These benchmarks assume paramount importance in the context of simulation testing, particularly for reactive protocols like the AODV protocol. Thus, these performance metrics are expounded upon in detail within the results section, encompassing crucial aspects such as packet delivery fraction, average end-to-end delay, and normalized routing load.

4.3.1 PACKET DELIVERY FRACTION SCENARIO

The Packet Delivery Fraction (PDF) metric gauges the proportion of packets successfully transmitted from the source node to the destination node. In Figure 3, a performance comparison is drawn among three protocols, considering the pause time against the PDF metric. In this scenario, the AODV protocol without dropped packets

remains consistent at 1.9871% across varied pause times, with one instance at 100 (indicating no motion) and another at 10 (approximating continuous motion). Contrastingly, the AODV protocol with dropped packets exhibits a notably reduced packet delivery fraction, standing at 0.8419%. In a contrary trend, the FS-AODV protocol manifests a heightened packet delivery fraction, recording an increment at 0.9873%. This enhancement is attributed to the persistent network activity and minimal downtimes, which influence the network's structural dynamics. Evidently, the overarching conclusion underscores the superior performance of FS-AODV in comparison to AODV, evident by the augmented data packet delivery rates.

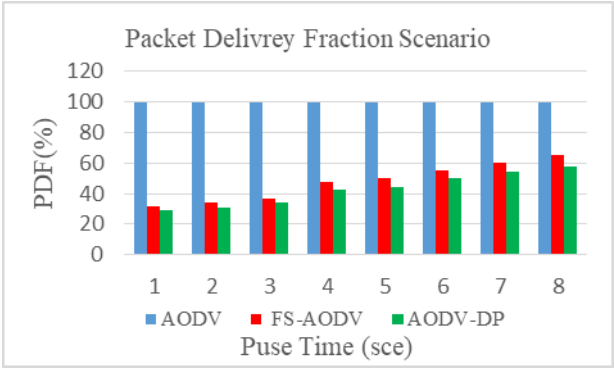

FIGURE 3. Packet delivery fraction scenario

4.1.2 AVERAGE END-2-END DELAY SCENARIO

The End-to-End (E2E) metric captures the average delay encountered by a data packet traveling from a source node to a destination node within the framework of a routing protocol.

Illustrated in Figure 4 is the impact of a pause time of 10 seconds, which generates an environment of almost continuous motion, subsequently rendering the network unstable and inherently influencing routing messages. Notably, the average end-to-end delay for the AODV protocol without dropped packets exhibits a marked high value of 0.0007%. Similarly, the AODV protocol with dropped packets also records a substantial delay rate, standing at 0.0005%. In general, for both instances of AODV—without and with packet drops—a limited number of Route REQuest (RREQ) and Route REPlies (RREP) messages are required by the source node when exploring new paths to the destination via the shortest route.

Conversely, the FS-AODV protocol displays a slightly elevated average end-to-end delay value, measuring at 0.0006%. This observed augmentation in delay can be attributed to network instability within this particular scenario.

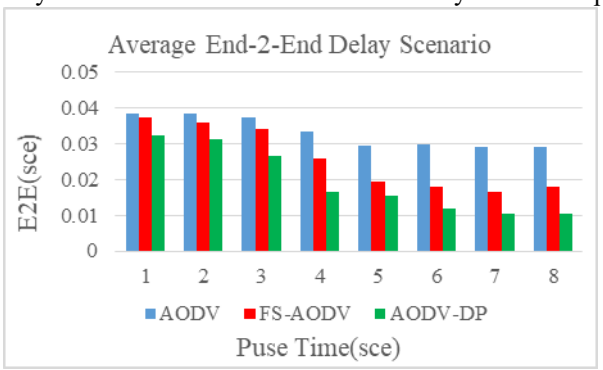

FIGURE 4. Average E2E Delay Scenario

4.1.3 NORMALIZED ROUTING LOAD SCENARIO

The Normalized Routing Load (NRL) metric gauges the rate of routing control packets successfully conveyed from source nodes to destination nodes across the network.

As depicted in Figure 5, a pause time of 10 seconds (reflecting continuous motion) engenders an elevated NRL due to fluctuating path alterations and heightened node mobility. Conversely, increasing the pause time to reach a state of "non-moving" results in a diminished value of normalized routing load due to the stabilized node movement. In this context, the source node dispatches Route REQuest Error (RRER) messages to explore routes and detect route disruptions. Consequently, it solicits routes and unveils novel pathways through the broadcasting of new Route REQuest (RREQ) messages.

Notably, the AODV protocol without dropped packets registers a high NRL at 0.0127%, attributed to the preference for the shortest route. Meanwhile, the AODV protocol with dropped packets also records a notable NRL at 0.066%,

arising from route alterations. Conversely, the FS-AODV protocol with dropped packets exhibits a heightened NRL at 0.058%, stemming from the selection of a dependable and efficient path from source to destination.
In sum, the outcomes underscore the commendable performance of FS-AODV with dropped packets vis-à-vis AODV with dropped packets, primarily evidenced by the PDF parameter's value.

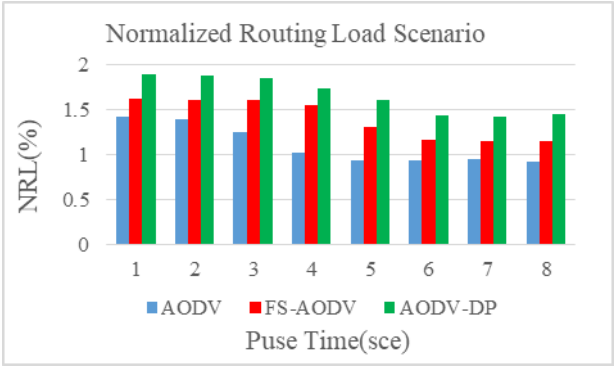

FIGURE 5. Normalized Routing Load Scenario

In conclusion, the outcomes across the three scenarios distinctly illuminate the impact of parameters on the reactive protocol within the MANET context. Notably, the enhanced FS-AODV protocol demonstrated commendable performance throughout the experiments in comparison to both AODV variants—without packet drops and with packet drops. This assessment is firmly substantiated by the observed values of the three critical parameters, namely PDF, E2E, and NRL.

4.2 PROPOSED MODEL VALIDATION

Incorporating benchmarking against other studies holds paramount importance in substantiating the credibility of the proposed model. In our research, a novel protocol was conceived through the fusion of the fuzzy system with the conventional AODV protocol, grounded in the principles of trust and hop counts. The empirical evidence unequivocally establishes that the developed FS-AODV model outperforms both AODV variants—without and with packet drops—across the metrics of PDF, E2E, and NRL.

In parallel, a study conducted by Shubham Choudhary et al. [24] adopted a similar approach, integrating a fuzzy system with the traditional AODV routing protocol, albeit based on five distinct parameters: speed, hop count, residual energy, bandwidth, and link expiration time. Notably, their findings corroborate the superiority of the fuzzy AODV protocol over the traditional AODV protocol across the metrics of Packet Delivery Ratio (PDR), End-to-End delay (E2E), and throughput.

This comparison with the other study unequivocally validates the efficacy of our proposed approach, despite some divergences in terms of the factors employed.

5 CONCLUSION AND LIMITATIONS

The domain of the Internet of Things (IoT) is still promising, especially when it comes to the wireless networks that use the MANET routing protocols. IoT's development influence is spread across different industries such as industrial, health, and education sectors, all of which are under wireless network systems. This research therefore emphasizes the use of artificial intelligence especially the use of a fuzzy system with the overall aim of enhancing the effectiveness of MANET protocols. This integration involved the synchronization of the fuzzy system with the reactive AODV protocol, with special emphasis on trust level and hop count. This synergistic approach gave rise to a novel algorithm called "FS-AODV" that is based on the principles of fuzzy logic. The findings provided a clear story on the improvement of the FS-AODV protocol over the normal AODV protocol – without and with packet drops – based on the three outlined parameters. With the progression of this study, a detailed analysis of the limitations and a more extensive assessment of the fuzzy system's applicability to MANETs could provide a richer understanding of the topic. This, in turn, could promote the development of new solutions based on artificial intelligence to maximize the efficiency of routing in the context of the dynamics of wireless networks and the IoT environment. Therefore, the subsequent projects can possibly include integration of the fuzzy system with various protocols in the context of the constantly evolving environment of MANETs, thus expanding the developments of the domain.

5.1 LIMITATIONS

Despite the tangible benefits of optimizing the proposed model which greatly enhanced the security and reliability of the routing protocols within the MANET-IoT environment, it is necessary to acknowledge several limitations that need to be taken into consideration:

- Computational complexity: Intelligent system integration, especially one involving fuzzy logic, may increase the computational overhead.
- Energy Consumption: The intelligent system's continual assessment of trust levels and route nodes could lead to increased resource consumption, including memory and battery life.
- Scalability Challenges: The proposed model demonstrates effectiveness within controlled scenarios, but its scalability to large-scale networks remains a concern.
- Network Dynamics: Rapid changes in network topology, such as node failures or sudden mobility changes, might lead to delays or inaccuracies in routing decisions, impacting the overall reliability of the protocol.
- Security Considerations: Security threats pose a major challenge, so the model should be evaluated against potential attacks, vulnerabilities, and countermeasures to ensure its robustness.

FUNDING:

None

ACKNOWLEDGMENT

The authors appreciate the support of the Scientific Research Committee at the University of Diyala for this great the research project, as well as some friends who provided their valuable advice to improve the quality of the research.

CONFLICTS OF INTEREST:

None

REFERENCES

[1] K. Divya and B. Srinivasan, “A Trust-Based Predictive Model for Mobile Ad Hoc Networks,” *Int. J. AdHoc Netw. Syst.*, vol. 11, no. 03, pp. 13–23, 2021, doi: 10.5121/ijans.2021.11302.

[2] J. Gowrishankar, P. S. Kumar, T. Narmadha, and N. Yuvaraj, “A Trust Based Protocol For Manets In Iot Environment,” *Int. J. Adv. Sci. Technol. Vol.*, vol. 29, no. 7, pp. 2770–2775, 2020.

[3] V. Suryani, S. Sulistyo, and W. Widyawan, “ConTrust: A trust model to enhance the privacy in internet of things,” *Int. J. Intell. Eng. Syst.*, vol. 10, no. 3, pp. 30–37, 2017, doi: 10.22266/ijies2017.0630.04.

[4] R. T. Merlin and R. Ravi, *Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET*, vol. 104, no. 4. Springer US, 2019. doi: 10.1007/s11277-019-06120-8.

[5] Q. M. Yas and M. Khalaf, “REACTIVE ROUTING ALGORITHM BASED TRUSTWORTHY WITH LESS HOP COUNTS FOR MOBILE AD-HOC NETWORKS USING FUZZY LOGIC SYSTEM,” *J. SOUTHWEST JIAOTONG Univ. Vol.54*, vol. 54, no. 3, pp. 1–11, 2019.

[6] Q. M. Yas and M. Khalaf, “A Trusted MANET Routing Algorithm Based on Fuzzy Logic,” *Commun. Comput. Inf. Sci.*, vol. 1174 CCIS, pp. 185–200, 2020, doi: 10.1007/978-3-030-38752-5_15.

[7] V. Jayalakshmi and T. Abdul Razak, “Trust based power aware secure source routing protocol using fuzzy logic for mobile adhoc networks,” *IAENG Int. J. Comput. Sci.*, vol. 43, no. 1, pp. 98–107, 2016.

[8] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen, and R. U. Ashraf, “Multi-hop interpersonal trust assessment in vehicular adhoc networks using three-valued subjective logic,” *IET Inf. Secur.*, vol. 13, no. 3, pp. 223–230, 2019, doi: 10.1049/ietifs.2018.5336.

[9] S. Muhammad, L. Wang, and B. Yamin, “Trust model based uncertainty analysis between multi-path routes in MANET using subjective logic,” *Commun. Comput. Inf. Sci.*, vol. 812, pp. 319–332, 2018, doi: 10.1007/978-981-10-8123-1_28.

[10] T. L. Pooja and M. Supreetha, *Automated Data Acquisition and Controlling System in Housing Line Using Internet of Things (IoT)*, vol. 98. 2020. doi: 10.1007/978-3-030-33846-6_1.

[11] N. Khanna and M. Sachdeva, “Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation,” *Int. J. Commun. Syst.*, vol. 32, no. 12, pp. 1–23, 2019, doi: 10.1002/dac.4012.

[12] W. Alnumay, U. Ghosh, and P. Chatterjee, “A trust-based predictive model for mobile Ad Hoc network in internet of things,” *Sensors (Switzerland)*, vol. 19, no. 6, pp. 1–14, 2019, doi: 10.3390/s19061467.

[13] G. M. Borkar and A. R. Mahajan, “A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks,” *Wirel. Networks*, vol. 23, no. 8, pp. 2455–2472, 2017, doi: 10.1007/s11276-016-1287-y.

[14] H. Xu *et al.*, “Trust-Based Probabilistic Broadcast Scheme for Mobile Ad Hoc Networks,” *IEEE Access*, vol. 8, pp. 21380–21392, 2020, doi: 10.1109/ACCESS.2020.2969447.

[15] M. Bharti, S. Rani, and P. Singh, "Efficient Cluster Head Selection and Trust Based Routing in MANET," *J. Phys. Conf. Ser.*, vol. 2327, no. 1, pp. 1–8, 2022, doi: 10.1088/1742-6596/2327/1/012049.

[16] A. Beghriche,and A. Bilami, "A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks," *Int. J. Intell. Comput. Cybern.*, vol. 11, no. 2, pp. 309–340, 2017.

[17] P. T. Kasthuri Bai, "RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET," *Int. J. Comput. Networks Appl.*, vol. 9, no. 2, pp. 150–159, 2022, doi: 10.22247/ijcna/2022/212331.

[18] K. A. P. Yamini, J. Stephy, K. Suthendran, and V. Ravi, "Improving routing disruption attack detection in MANETs using efficient trust establishment," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 5, 2022, doi: 10.1002/ett.4446.

[19] P. Networking and P. Periasamy, "Cluster and angular based energy proficient trusted routing protocol for mobile ad-hoc network," no. September, 2022, doi: 10.1007/s12083-022-01340-5.

[20] P. Sarao, "F-EEAODV: Fuzzy based energy efficient reactive routing protocol in wireless ad-hoc networks," *J. Commun.*, vol. 13, no. 7, pp. 350–356, 2018, doi: 10.12720/jcm.13.7.350-356.

[21] G. Xia, C. Yu, and J. Chen, "A Fuzzy-Based Co-Incentive Trust Evaluation Scheme for Edge Computing in CEEC Environment," *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312453.

[22] M. N. Doja, B. Alam, and V. Sharma, "Analysis of Reactive Routing Protocol Using Fuzzy Inference System," *AASRI Procedia*, vol. 5, pp. 164–169, 2013, doi: 10.1016/j.aasri.2013.10.073.

[23] T. Tashtoush, A. Alazzam, and A. Rodan, "Utilizing fuzzy logic controller in manufacturing facilities design: Machine and operator allocation," *Cogent Eng.*, vol. 7, no. 1, pp. 1–16, 2020, doi: 10.1080/23311916.2020.1771820.

[24] M. Faiz and S. Pramanik, *Software Defined Networking for Ad Hoc Networks*, no. February. 2022. doi: 10.1007/978-3-03091149-2.