Secure data transmission in mobile Ad-hoc network using Multi-path routing techniques

Jayantkumar A Rathod[1], Abhishek S V[2], Anand M R[3], C H Rakesh[4], and Poorvika B M[5]
{jayant1977@aiet.org.in, abhiachar86@gmail.com, anandmr8123@gmail.com, chilakurirakesh74117@gmail.com, 4al20is035@gmail.com}
[1]Department of ISE, Alvas Institute of Engineering and Technology, Mijar.
Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

Abstract - Mobile Ad-hoc Networks (MANETs) are dynamic and decentralized, they pose special issues for securing data transfer. Traditional routing systems struggle to deliver dependable and secure communication in such settings. This research provides a novel approach that uses multi-path routing algorithms to improve the security and reliability of data transmission in MANETs. The suggested system dynamically creates numerous paths between source and destination nodes, taking advantage of MANET's inherent redundancy to offset the consequences of node failures and malicious attacks.
Each path is chosen based on criteria such as link stability, residual energy, and security parameters to ensure robustness and privacy. Furthermore, cryptographic techniques are used to encrypt data packets, preventing eavesdropping and tampering while transmission. Furthermore, authentication procedures have been implemented to check the Simulation results demonstrate the effectiveness of the proposed approach in improving data transmission security while maintaining acceptable performance metrics such as throughput, latency, and packet delivery ratio. The multi-path routing strategy enhances network resilience against attacks and node failures, making it suitable for deployment in MANETs operating in hostile or unpredictable environments.

Keywords - *AD-HOC, MANET, AODV, CH, Quality of service, Real Time traffic.*

1 INTRODUCTION

Developed for Mobile Ad hoc Networks (MANETs), TriChain is a sophisticated intrusion detection system that uses kangaroo-based techniques to improve the security of multipath route discovery and management. It combines cluster-based architecture with cutting-edge routing protocols to improve network efficiency, scalability, and resilience while guaranteeing stable performance under demanding and changing conditions [1].

Mobile Ad-hoc Networks (MANETs) are decentralized networks made up of mobile devices that connect with one another without the need for a permanent infrastructure. They find use in a variety of settings, including military operations, disaster aid, and vehicle communication systems. However, due to their dynamic topology and lack of centralized management, MANETs are vulnerable to a variety of security risks, including as eavesdropping, data tampering, and denial of service attacks.

Ensuring safe data transmission in MANETs is difficult due to their intrinsic characteristics, such as node mobility, limited resources, and unpredictable network conditions. Traditional routing protocols, such as AODV (Ad-hoc On-demand Distance Vector) and DSR (Dynamic Source Routing), were not developed with security in mind, and therefore may be subject to spoofing, black hole, and wormhole attacks.

To solve these issues, researchers offered a variety of security techniques and routing strategies. One interesting option is to use multi-path routing algorithms, which provide numerous paths between source and destination nodes to improve dependability and security. Multi-path routing reduces the impact of node failures, congestion, and malicious assaults by spreading data across numerous channels.

This work presents a complete analysis of safe data transmission in MANETs using multi-path routing algorithms. We investigate the benefits of multi-path routing for increasing data secrecy, integrity, and availability in dynamic ad-hoc networks. In addition, we examine the integration of cryptographic algorithms and authentication systems to improve data transmission security.

2 RELATED WORK

Developed for Mobile Ad hoc Networks (MANETs), TriChain is a sophisticated intrusion detection system that uses kangaroo-based techniques to improve the security of multipath route discovery and management. It combines cluster-based architecture with cutting-edge routing protocols to improve network efficiency, scalability, and resilience while guaranteeing stable performance under demanding and changing conditions [1].

A study conducted in May 2000 presents a flexible quality of service model designed for ad hoc networks [9]. Focusing on quality-of-service aspects, the model aims to improve overall performance and reliability in dynamic network environments.

The second study investigates the implementation of real-time on-demand distance vector routing in a mobile Ad-hoc application. networks Emphasizing the requirements of real-time communication, the study addresses the challenges of timely data delivery in dynamic network scenarios [10].

The study investigates an energy-based and link-state-based mechanism for AODV routing requests in mobile advertising hoc networks. Considering energy efficiency and network conditions, the study aims to optimize routing decisions to improve performance and resource utilization [11].

In a study by Li Ting, TANG Rui-bu and Ji Hong (2008), the article proposes a space. adaptive routing method with delayed retransmission method, especially for AODV-based MANETs. By dynamically adapting routing strategies based on network state, research aims to improve routing efficiency and adaptability in dynamic network environments [12].

The work "Performance Analysis of MANET Routing Protocols for Multimedia Traffic" performs a performance analysis of different MANET routing protocols with a focus on multimedia traffic. Analysing the effectiveness of different protocols to support multimedia data transmission, the study provides insight into the optimization of data transmission for different data types in mobile Ad-hoc networks [14].

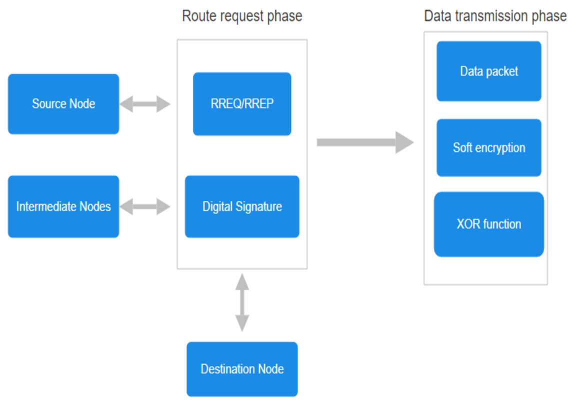
M. Gunes and M. Wenig present the 2009 work. models of realistic mobility patterns and radio wave propagation characteristics in Ad Hoc network simulations. By combining realistic mobility and propagation models, the study aims to improve the accuracy and reliability of network simulations to better understand network behaviour in dynamic environments [15].

Another study conducted in 2010 introduces a quality of service (QoS) routing protocol tailored for mobile Ad Hoc networks with a focus on load sharing. Considering load balancing and QoS requirements, the protocol aims to optimize routing decisions to improve network performance and resource utilization [13].

A study by Iftikhar Ahmad, Humaira Jabeen and Faisal Riaz in 2011 found that quality of service (QoS) routing is improved offered access is specially adapted for real-time traffic in mobile Ad Hoc networks. Focusing on real-time communication requirements, the study aims to optimize routing decisions to ensure timely and reliable data delivery under dynamic network scenarios.

3. PROPOSED WORK

Based on our in-depth study of route discovery algorithms and Mobile Ad-hoc Networks (MANETs), we have created a comprehensive set of protocols for putting our methodology into practice. Our methodology focuses on integrating different methodologies, including Cluster-based Multipath Routing Algorithm, AODV, MBOMRP, and RREQ, etc, to optimise route discovery and maintenance.



In our proposal, we outline specific steps which include:

Figure 3.1 Block diagram of the proposed protocol

3.1 Cluster Formation

In Mobile Ad-hoc Networks (MANETs), cluster formation is an essential process where in nodes self-organize into logical groupings or clusters according to factors such as energy levels, proximity, and connectivity. The coordination and management of networks is improved by this organisation. Node selection, cluster head election, and stability and communication range considerations are all part of the cluster building process. Once established, clusters need to be maintained to adjust to changes in the network and maintain reliable communication both inside and across clusters. Large-scale and dynamic MANET environments are supported by dynamic approaches and hierarchical clustering. In MANETs, efficient cluster creation maximises scalability, communication effectiveness, and resource utilisation.

3.2 Selection of Cluster Head

In Mobile Ad-hoc Networks (MANETs), cluster head election is an important procedure where nodes choose a central coordinator according to factors including connection and energy levels. In order to ensure effective network functioning and resource utilisation, the elected cluster head oversees intra-cluster communication and acts as a gateway for inter-cluster communication.

To identify the CH, a Cluster Head Selection Algorithm (CHSA) is integrated into the approach described. The maximum energy of nodes and the dependability pair factor are used by this approach to calculate the CH. The node with the greatest energy level is identified as the Cluster Head (CH), while the other nodes are designated as backup Cluster Heads. These backup cluster heads perform two important tasks: first, they take over as CH when the primary's energy runs low, and second, a backup SCH is used to handle CH failures.

The Cluster Head Selection Algorithm (CHSA) is outlined as follows:

- Specifications Calculation: Using the parameters Node Energy (N_E), Node Distance (N_D), and Fault Ratio Probability (F_RP) in relation to the base station, get the Cluster Head (CH). As the CH, pick the node with the highest N_E, N_D, and lowest F_RP values.
- Request Message Broadcast: Send out a request message (REQ) to every node in the network as soon as the CH has been located. Similar route nodes recognise the REQ and react appropriately.
- Fault Ratio Probability Computation: Compute F_RP using the formula F_RP =
- Selecting an Alternative Cluster Head: Based on priority, choose an alternative cluster head (SCH) following the identification of the CH. CH > SCH > Nodes of Members (MN). The stability pair(Ep^rem * Eq\rem) / d(p, q, t), where d(p, q, t) represents the distance between nodes p and q at a given timestamp t, and Ep\rem and Eq\rem represent the remaining energy levels of nodes p and q, respectively

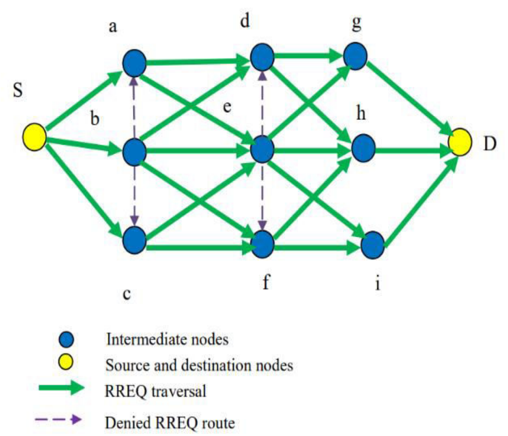
factor, distance, and energy availability are taken into account when selecting SCH.

- Routing Table Update: To enable effective communication among cluster members, the CH updates the base station's routing table, which contains data about each member.
- Substitute Cluster Head Management: In the event that the CH post becomes open, the energy, distance, and stability pair factor of the cluster members are managed by the substitute CH.
- Finding the Most Efficient Path: Choose the least number of hops between the base station and the CH, as well as between the CH and group nodes, while taking into account the greatest energy availability.

3.3 Route Discovery Process

• The routing process uses the Ad hoc On-Demand Distance Vector (AODV) routing protocol.

• The routing process is initiated by a source node that needs to communicate with a destination node but does not yet have a route defined.



• When requesting information about a destination or its route, a source node sends a Route Request packet (RREQ) to surrounding nodes.

• Route Reply (RREP): A Route Reply packet with route information is sent back to the source node when the RREQ reaches the destination node or nodes. who is aware of the way to the goal.

Figure 3.3.1 Route discovery

• Forwarding RREQ: If they do not have information about the destination or already

3.4 Multipath Selection

The cluster head or intermediate nodes examine their routing tables after receiving the RREQ in order to determine the best possible multipath route to the destination. Many criteria, including hop count, available bandwidth, and network reliability, are taken into consideration while choosing paths.

3.4.1 Mobility-Based Path Selection (MBOMRP)

• Nodes constantly monitor their own and the movement space of their neighbours.
• Nodes update their mobility information about both source and destination nodes by receiving Route Request (RREQ) packets.
• This includes heading, speed, stability indicators and other relevant features.
• Based on movement information, nodes evaluate possible paths for stability and reliability.
• When creating multiple routes, routes with greater stability and reliability are preferred.
• Selection criteria can be, for example, lower speed, better stability and fewer nodes.

3.5 Route Maintenance

In Mobile Ad-hoc Networks (MANETs), route maintenance is essential because it ensures communication pathways remain reliable in the face of constantly shifting network circumstances. It requires constant connection quality monitoring, quick failure diagnosis, and appropriate tweaks to maintain effective routes. By utilising techniques like route error detection, reconstruction, and periodic updates, MANETs are able to adjust to changes in topology in real time, so that communication remains stable and robust. To ensure that well-traveled routes remain accessible, AODV effectively oversees route maintenance. A node transmits a Route Error (RERR) packet to the source node when it detects a route failure, such as a broken link or node migration. The source node starts a fresh route discovery process to look for an alternate path after receiving the RERR message.

3.6 Packet Forwarding

- Mobile Ad-hoc Networks (MANETs) rely on packet forwarding, a fundamental networking method that enables nodes to efficiently send data packets between source and destination nodes.
- Data Packet Transmission: Data packets leave the source node and follow a number of predetermined paths to their destination.
- Forwarding Decisions: Based on data from the node's routing table, sequence numbers, and the particular pathways selected for packet transmission, forwarding decisions are determined at each intermediary node along the path.
- Packet Reassembly and Acknowledgment: If packets is/are broken during the transmission, it can be reassembled when it reaches the destination node. Data is sent in an orderly and reliable manner because the destination node informs the source node that the packets have been received.

3.7 Destination Reception

After data packets arrive at their destination and are handed over to the intended receiver, the transmission process is concluded.

4. SIMULATION RESULTS

4.1 Simulation setup

The dynamic behaviour of communication networks is Network Simulator (NS), a discrete event-driven network simulation tool. A lot of support is offered by Network Simulator 2 (NS2) for simulating various protocols via wired and wireless networks. For wired and wireless simulations, it offers a highly modular framework that supports various network elements, protocols, traffic patterns, and routing styles. TCP, UDP, HTTP, and DHCP are among the network protocols that can be simulated with the help of the simulation software NS2.

Parameters	Values
Simulation time	900 sec
Number of mobile nodes	50 nodes
Max speed of monile node	20 m/s
Area size	1500mX3000m
MAC	IEEE 802.11
Propagation mode	Two ray ground
Node mobility	Random
Traffic	Constant bit rate (CBR)
Agent	UDP
Queue length	50 bytes
Number of sources	1, 3, 5, 7
Pause time	0s, 10s, 20s, 30s, 40s, 50s

Table 1 Simulation parameters

Additionally, this package makes it simple to generate a variety of network traffic types, including available bit rate (ABR), variable bit rate (VBR), and constant bit rate (CBR). In academic settings, this simulation tool is highly well-liked.

4.2 Results

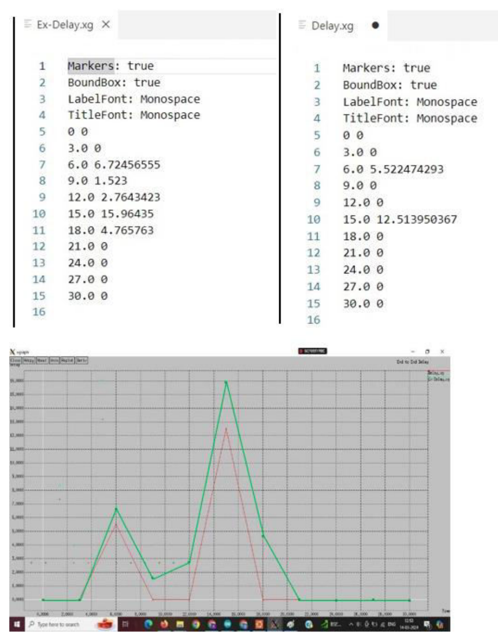


Fig. 4.2.1 Packet Delay

In the above graphical representation of delay over time, the green line denotes previous packet delay, while the red line signifies present packet delay. It's evident that there has been a decrease in packet delay compared to the previous data.

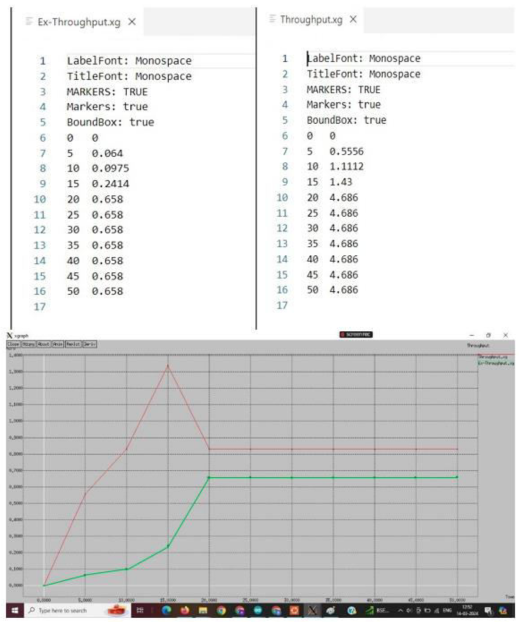


Fig.4.2.2 Throughput

In the graph, the green line reflects past throughput, while the red line indicates current throughput. Remarkably, the current throughput surpasses that of the previous data.

5. FUTURE ENHANCEMENT

In dynamic network contexts such as MANETs, integrating multipath routing with hybrid encryption algorithms provides a strong approach for improving data security. This method protects confidentiality and integrity during transmission by combining symmetric encryption (like AES) for effective bulk data encryption and asymmetric encryption (like RSA) for safe key exchange. By addressing important security issues, this integration strengthens the dependability and robustness of communication channels in intricate network environments channels

6. CONCLUSION

We created a protocol with an improved route finding technique that lowers the pre-transmission latency by avoiding the RREQ rejection. EAODV prioritises the RT transmission source node. For RT transmission, when an RREQ packet is sent to a neighbouring node, it initiate the RT transmission after prioritising the acceptance of route requests. The number of packets dropped decreased, and as more packets arrived at their destination, throughput climbed along with the delivery ratio. Our method is to keep the communications going in real time. Compared to the standard AODV routing system, our protocol's improvements improve the network's overall throughput and the packet delivery ratio for real-time transmission. The outcome of the simulation demonstrates how the protocol's performance has improved.

7. REFERENCES

[1]. Jayantkumar A Rathod, Manjunath Kotari, “TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol”, International Journal of Computer Networks and Applications (IJCNA), 11(1), PP: 61-81, 2024, DOI: 10.22247/ijcna/2024/224436.

[2]. S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance issues and Evaluation Considerations”, Network Working Group, RFC2501, January 1999.

[3]. C. Perkins, E. Belding Royer and S. Das “Ad hoc on-demand Distance Vector (AODV) Routing” IETF RFC3561, July 2003.

[4]. Iftikhar Ahmad & Mata ur Rehman“Efficient AODV routing based on traffic load and mobility of node in MANET” 6th International Conference on Emerging Technologies (ICET),2010.

[5]. Iftikhar Ahmad & Humaira Jabeen “Enhanced Load Balanced AODV Routing Protocol” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 9, No. 1,January 2011.

[6]. Abdullah waqas, shahid Imran & hasan mahmood"Energy Efficient Route Discovery for Reactive Protocols in Wireless Ad Hoc Networks", 2012 International Conference on Emerging Sciences (ICET),8-9 Oct. 2012.

[7]. Nisar Hundewale, Sunsook Jung & Alex Zelikovsky "Energy Efficient Node Caching and Load Balancing Enhancement of Reactive Ad Hoc Routing Protocols" Journal of Universal Computer Science, vol. 13, no. 1 (2007), 110-132.

[8]. Mrs.Shilpi Jain, Mr.Sourabh Jain "Energy Efficient Maximum Lifetime Ad-Hoc Routing(EEMLAR)", IRACST–International Journal of Computer Networks and Wireless Communications(IJCNWC),ISSN:2250-3501 Vol.2, No4, August 2012.

[9]. Iftikhar Ahmad,Humaira Jabeen & Faisal Riaz, "ImprovedQOS Routing for Real Time Traffic in Mobile Ad hoc Network"International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.4,July 2013.

[10]. H. XIAO, Winston K.G. SEAH, Anthony LO and Kee Chiang CHUA "Flexible Quality Service Model for Ad-HOC Networks" In proceedings of the IEEE Vehicular Technology Conference, Tokyo, Japan, May 2000.

[11]. Sanjeev Jain, Venkateswara Pitti and Bhupendra Verma. "Real Time On-demand Distance Vector in Mobile Ad hoc Networks" Asian Journal of Information Technology 5(4): 454-459, 2005.

[12]. Li Hao Jutao, Zhao Jingjing and Minglu, "Energy Level and Link State Aware AODV Route Request Forwarding Mechanism Research" WSEAS Transactions on Communications, Issue 2, Volume 8, February 2009.

[13]. LI Ting, TANG Rui-bu and JI Hong,"Status adaptive routing with delayed rebroadcast scheme in AODV-based MANETs" Science Direct, September 2008 Elsevier.

[14]. P.Sivakumar , Dr.K.Duraiswamy Research Scholar "A QOS Routing Protocol for Mobile Ad Hoc Networks based on the Load Distribution"IEEE International Conference on Computational Intelligence and Computing Research (iccic'10) 2010.

[15]. Chhagan Lal, V.Laxmi, M.S.Gaur "Performance Analysis of MANET Routing Protocols for Multimedia Traffic" International Conference on Computer & Communication Technology (ICCCT)-2011.

[16]. M. Gunes¸ and M. Wenig, "Models for Realistic Mobility and Radio Wave Propagation for Ad Hoc Network Simulations" Springer-Verlag London Limited, 2009. (A chapter of book "Guide to Wireless Ad Hoc Networks").

[17]. K. Fall and K. Varahan, editors, "NS Notes and Documentation" The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, November 1997.

[18]. Rajesh Verma, & Priya Sharma. "Efficient Intrusion Detection Systems for Mobile Ad-hoc Networks." (2019), International Journal of Network Security & Its Applications (IJNSA).

[19]. Sanjay Patel, & Meena Gupta."Trust-Based Routing Protocols for Secure Communication in Mobile Ad-hocNetworks."(2017),International Journal of Computer Networks & Communications (IJCNC).

[20]. Deepak Kumar, & Pooja Singh. "Cross-Layer Design Approaches for Enhancing Security in Mobile Ad-hoc Networks." (2018), International Journal of Wireless & Mobile Networks (IJWMN).

[21]. Ananya Mishra, & Vikas Choudhary. "Behavioral Analysis Techniques for Anomaly Detection in Mobile Ad-hoc Networks"(2016), International Journal of Computer Science and Information Security (IJCSIS).

[22]. Ravi Sharma, & Nisha Verma. "Secure Data Aggregation Schemes for Wireless Sensor Networks in Mobile Ad-hoc Environments." (2015),

International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC).