SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X Volume 4, Issue 6, 2026

ENHANCED ROUTE VALIDATION MECHANISM TO MITIGATE THREE-NODE INSTABILITY IN ROUTING INFORMATION PROTOCOL

Younas Iqbal[1], Iqra Khan[2], Shah Khalid[*3], Muhammad Salam[4], Haseena Noreen[5], Aftab Alam[6], Fakhrud Din[7]

[1,2,*3,4,5,6,7]*Department Of Computer Science and IT, University of Malakand, Pakistan*

[*3]shahkhalid@uom.edu.pk

DOI: https://doi.org/10.5281/zenodo.20745978

Keywords
RIP, Distance vector protocol, Routing,3-Node instability

Article History
Received: 21 April 2026
Accepted: 03 May 2026
Published: 18 June 2026

Corresponding Author: *
Shah Khalid

Abstract
The three-node instability problem of the Routing Information Protocol (RIP) is examined in this study as one of the manifestations of the count-to-infinity problem in distance vector routing protocol, which is crucial in this context. Although the split-horizon as well as the poison reverse are effective in the case of two node instability causes by the loops, they do not stop routing loops in case of three nodes and thus delay convergence and deteriorate the performance of the network. In order to counter this shortcoming, the solution of verification is suggested, according to which routers verify alternative routes with the original source before accepting them. This helps to avoid the spread of the outdated or misleading updates and provides stable routing decisions. The method proposed is demonstrated with the help of a detailed example based on Forouzan Data Communications and Networking with the flowcharts, pseudo-code, and graphical simulation. After comparative analysis, it can be seen that, verification-based method has a higher convergence rate, ensures that loops are avoided, and is more stable than simple distance vector routing and split horizon with poison reverse. The results identify the efficiency and feasibility of the presented solution, and further effort recommends the expansion of the mechanism to bigger topologies, incorporation of the newest protocols and the use of intelligent algorithms to enable proactive loop recognition.

1. INTRODUCTION

Data communication is the process of exchanging data between communicating devices through guided or unguided media. Protocols that have been agreed upon to ensure accurate and precise information exchange. The data transfer uses protocols and communication channels between two points [1]. Connecting devices, including computers, printers, and other equipment with the capability to send and receive information is known as networking [2]. The art of networking involves connecting computers that work together and other devices to communicate through channels to share resources, data, and services [3]. It uses switches, routers, and transmission media (such as cables or Wi-Fi) to transport and transmit data. Protocols are used to create rules such as TCP/IP. Network services simplify and facilitate communication. Security measures ensure data security. Network interface activation (e. g.,NIC card or Wi-Fi adapter) enables the network to participate[4]. Switches are used between devices within the same network, whereas routers connect various networks and direct data to the appropriate location. The exchange of information is structured in accordance with

special rules known as protocols (such as TCP/IP) to enable all devices know each other. For making the Networks become more helpful with email and file sharing, Additional network services like DNS(naming) and DHCP(automatic IP addresses) are used. Firewalls and other network security encryption tools help prevent hackers or misuse of data. All these parts together create a system that enables communication and sharing of resources [5].

1.1 Application of networking

The applications of networking are widespread across nearly all areas of contemporary life, enabling seamless operation, efficient information exchange, interaction, and cooperation between people, organizations, and machines. Networking plays a vital role in the following sectors:

- **Business sector,** Networking helps companies connect employees and share data, storage devices, and printers through centralized data management systems. These systems enhance productivity and reduce operational costs. Corporate networks also support applications such as email systems, video conferencing, enterprise resource planning (ERP), and cloud-based collaboration tools, enabling real-time teamwork across geographical boundaries [6].
- **Education,** Networking plays a critical role in enabling e-learning platforms, online courses, and remote access to educational resources. It allows students and teachers to communicate and collaborate regardless of their physical location [7].
- **Healthcare** The healthcare sector heavily relies on networking for telemedicine, remote patient monitoring, and electronic health record (EHR) systems, which improve patient care and increase accessibility to medical expertise [8].
- **Public services and Government,** Government and public service databases are managed through networked systems. Networking supports communication systems and security infrastructure, ensuring efficient communication between public administration and emergency response services [9].
- **Entertainment and media,** Streaming services, online gaming platforms, and digital media distribution rely on robust network infrastructures to deliver high-quality content to users worldwide.
- **Industrial applications,** Manufacturing industries employ networking for process automation, machine-to-machine communication (M2M), and Internet of Things (IoT) systems to monitor and control equipment remotely [10].
- **Transportation sector,** The transportation industry uses networking in intelligent transportation systems (ITS), GPS-based positioning, roadside control systems, and communication between autonomous and self-driving vehicles [11].

1.2 Routing and Routing Protocols

Routing refers to the process of identifying and selecting the most efficient path for data packets to travel between sending and receiving devices within a network. It ensures that information goes to its destination by the most appropriate methods [12]. The rules and algorithms that routers follow to exchange network information are known routing protocols that automatically determine optimal path of data. Examples are RIP, OSPF and BGP, which assist routers are dynamic with regards to changes in the network and do not need manual set up. Routing protocols ensure that data transfer is accurate, efficient and dynamic [13][14].

1.3 Problem Statement

RIP is a popular distance-vector protocol which has several limitations including two-node and three-node instabilities. In three-node instability, three routers form a cycle and create a routing loop, which leads to count to infinity situation, making the network unstable. Which causes routing oscillations and inefficiencies [15]. Existing mitigation techniques like split horizon and poison reverse can resolve the two-node instability, but they're inadequate for three-node instability problem. To solve this issue, we propose a solution of enhanced route validation to overcome the three-node instability problem in

RIP, which helps loop prevention, improve stability, faster convergence and optimized path.

1.4 Aim and Objectives

The main aim of the research will be to find out the limitations of the RIP protocol and to address the Three-Node instability issue to enhance the efficiency and stability of the network. The aim of our research will be accomplished with the following objectives:

i. To analyze the Three-Node Instability problem.

ii. To propose a solution to the Three-Node Instability Problem.

iii. To simulate and evaluate the proposed solution and measure its performance in terms of convergence time, packet loss and routing efficiency.

1.5 Plan of Work

To achieve the above objective, we have proposed a solution to address the three nodes in stability problem, incorporating strategies to prevent routing loops and enhance stability in dynamic topologies. The solution will be analyzing the three node instability problem of writing the pseudo-code and flowchart diagram in lucid chart. The implementation has been carried out in Python/C++ language. Following this, we have implemented and tested the proposed solution of using network simulation tools (Packet Tracer/NS-2, etc.) under varying scenarios with performance metrics such as convergence time, packet loss and routing efficiency. Finally, the work has concluded with recommendations for deploying the proposed solution in suitable applications and suggestions for future research to enhance distance vector routing protocols. The plan of work is shown in Figure 1.

Figure 1: Plan of Work

2. Literature Review

The process of choosing the most effective way for data to move across a network is called routing to a destination device from a source device. In computer networks information is divided into small packets or units that are transferred using the interconnected devices like routers and switches. When a packet is reaching to the final destination it may went through many in-between nodes, and routing decides the path that such packets should take. The decision-making Routing process is a process which is headed by a set of rules and algorithms which take into account factors such as network topology, link costs, congestion and reliability. In the absence of routing, data would not be transportable wisely over the complex networks like the internet which is literally a huge web of sub-networks that linked together [16]. One of the key computer networking operations is routing that facilitates movement of data among a sending device and the target recipient through a network of connections. Advance communication network are getting bigger and more complicated. This has consequently required routing dependabil-6ity and effectiveness of scheme. Facilitating efficient data transfer reducing latency and optimizing network utilization [17].The best route selection is carried out on the routing table using the routing algorithms. Administrative rules/regulations are

used for information sharing and topological change adaptation in the router's configuration. Both packet forwarding and other processes are based on routing as well as the flexibility, scalability and resilience of the modern Internet throughout the world. The response to the need to speed up communications, cloud computing real-time applications and the Internet of Things become clouded. Internet of Things routing protocols are supposed to be swift besides precise and credible convergence in addition to failure resilience [18]. Due to this, routing is an important field of study. It is especially in the business and academic sectors that it is addressed with issues such as convergence delays, scalability issues, security vulnerabilities and routing loops. Routing protocols such as distance vector routing protocols and link-state routing protocols are available which are typically divided into path-vector protocols and groups, having a unique design that can be used in certain environments.[19].For instance the Routing Information Protocol (RIP) is an early protocol that was essential to small businesses and medium-sized networks. Despite their drawbacks including count-to-infinity and routing instabilities issues. Higher-level protocols such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF) and Link-state were introduced to improve scalability and convergence [20]. Meanwhile, the Border BGP (Gateway Protocol) was now the inter-domain routing backbone, which dealt with the policies and complications of the world Internet. Although these have been made, there are differences between protocols compromises between scalability, complexity and stability, which has been the source of constant research toward optimization. The current literature review addresses the principles of routing, different kinds of routing, routing protocols and a critiquing of routing protocols. It brings out the strengths and Vulnerabilities of the most popular protocols, and especially, the RIP and the problem of its instability, which are still a problem in distancevector routing. Routing has evolved through the years and can be analyzed. The review provides the necessary theoretical foundation for retrospective data on RIP addressing in terms of methodologies and methods of use. Discussing possible opportunities and the three-node instability research problem. Improvements to give the protocol greater stability and efficiency [21].

3. Results and Discussion

3.1 Why we choose RIP while it is replace by many advance protocols?

Even though the Routing Information Protocol (RIP) is considered outdated, it still has practical applications in certain scenarios. It is commonly used in small and simple networks, such as offices, labs, or campus mini-networks, where the number of routers is limited and the topology is straightforward, because it is easy to configure and maintain. RIP is also widely used in academic and research environments, including universities and network simulations (e.g., Packet Tracer, GNS3, or Cisco Modeling Labs), as it helps students and researchers understand fundamental routing concepts such as distance-vector mechanisms, routing loops, and convergence behavior. Additionally, RIP serves as a baseline protocol for testing and prototyping new algorithms or stability improvements, like the ERVM model, due to its simple and predictable behavior. Some legacy networks or older devices continue to run RIP where upgrading is unnecessary or costly. Rarely, RIP is also configured as a secondary or backup routing protocol, providing basic routing if the primary protocol fails. The contribution of this research extends beyond RIP itself. The instability issues addressed in this work are fundamental to distance-vector routing and can also manifest in other routing environments under certain conditions. Therefore, the ERVM approach provides a conceptual framework that can be adapted and extended to more advanced protocols. In conclusion, RIP is selected not for its modern-day deployment relevance, but as a simplified experimental platform that enables effective validation of ERVM while maintaining the potential for broader applicability in complex routing systems.

3.2 Problem statement

Let's say that node A notifies B and C via packet that X is not reachable. Node B instantly updates its table, although the packet to C is lost in the network and never gets to C. Node C stays in the dark and continues to believe that there is a path to X via A with the cost of 5. The route to X is included in the routing table that node C eventually sends to B. Node B is totally fooled here. After receiving the route to X from C it updates its table based on the algorithm displaying the 8-cost route to X via C. Since C provided this information rather than A. Node B may eventually promote this path to A. At this point A is tricked and adds A to its table indicating that A can access X through B at a cost of 12. Naturally, the loop repeats, this time A advertises route to X to C at higher cost but not to B. Node C in turn advertisement routes to B at higher cost. Node B does the same to A. And so on. The loop is ended when the cost in the node becomes infinite.[15] as shown in (Figure 2).

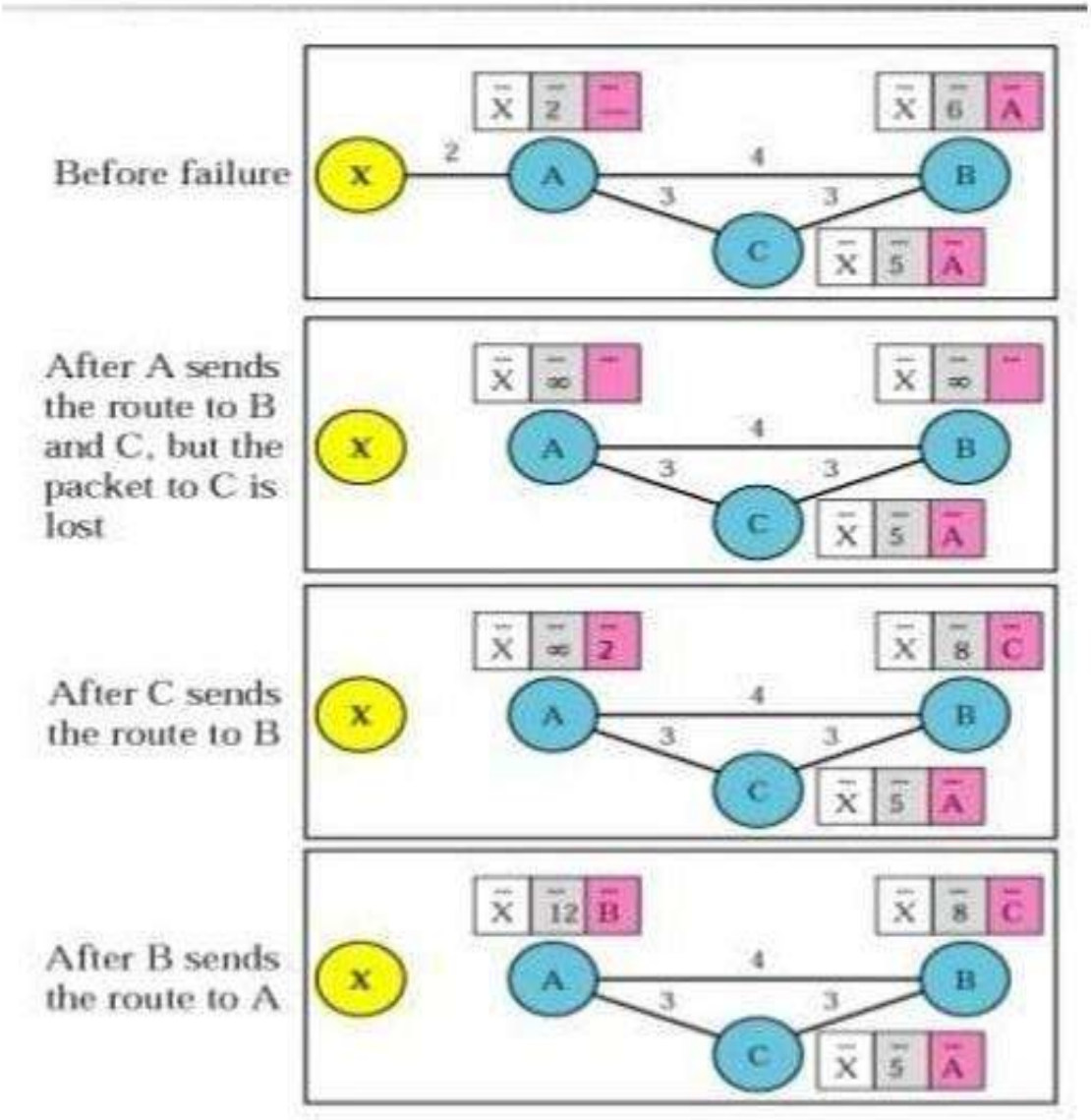

Figure 2: Three-node loop instability

3.2 Flowchart diagram of problem statement

Flowchart of problem statement is shown in Figure 3.

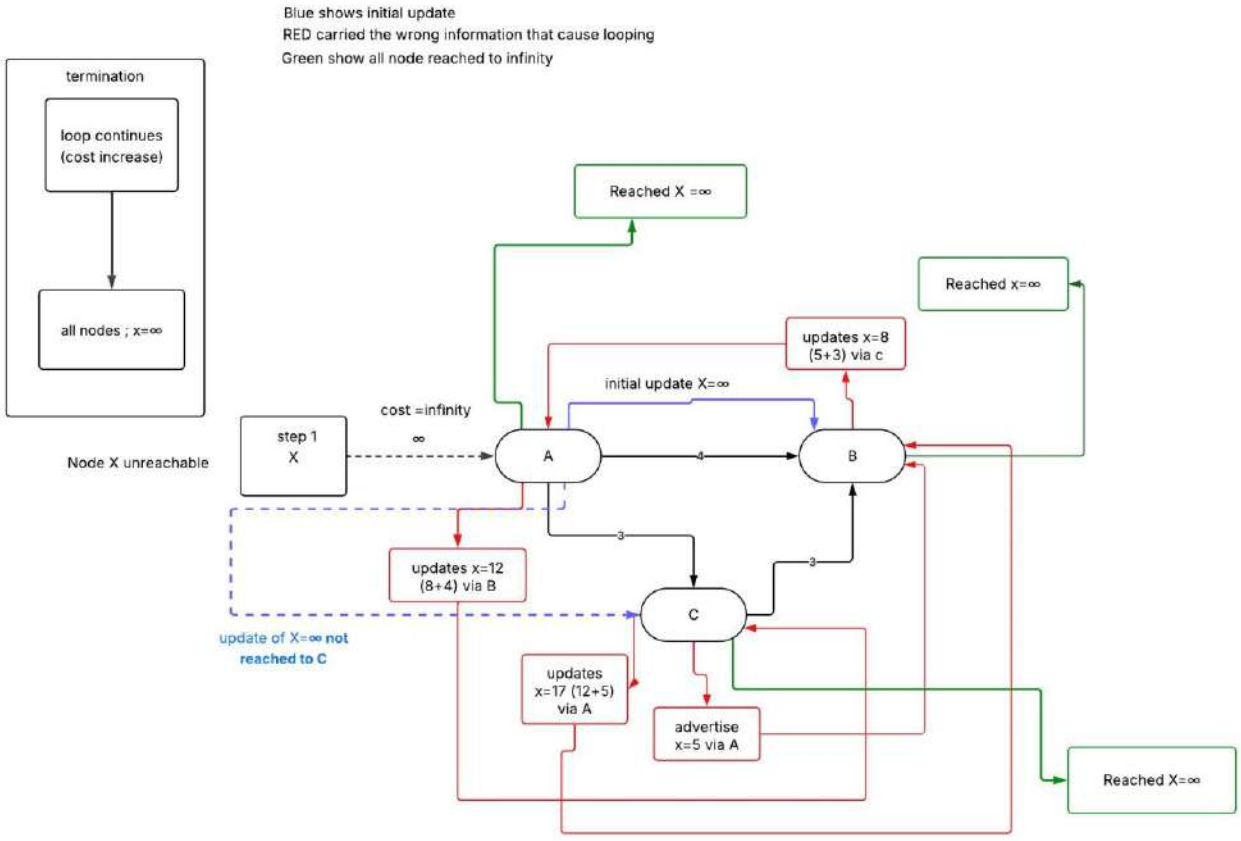

Figure 3 : Flow-chart of problem statement

3.3 Flowchart Description:

Initial Costs and Routes Setup:
Node X → Node A: Cost = 2
Node A → Node B: Cost = 4
Node A → Node C: Cost = 3
Node C → Node B: Cost = 6
Node B reaches X via A with Cost = 6 (2 + 4) •
Node C reaches X via A with Cost = 5 (2 + 3)
X becomes unreachable:
Node A detects that X is unreachable and sets Cost = infinity.
A informs B and C:
Node A sends update packets to B and C, informing them that X is
unreachable
B updates, C packet lost:
Node B receives the packet and updates its routing table to set Cost to X
= infinity.
The packet to Node C is lost, and C still has a Cost to X = 5.
C sends routing table to B:
Node C sends its routing table to B, which shows Cost to X = 5 via A.
B is fooled and updates its table:
Node B updates its routing table to show Cost to X = 8 via C (5 + 3).
B advertises to A:
Node B advertises the route to X via C with a cost of 8 to Node A.
A updates and is fooled:

Node A updates its table and shows Cost to X = 12 via B (8 + 4).
A advertises to C:
Node A advertises this route to X with a cost of 12 to C.
C updates and increases cost:
Node C updates its routing table and shows Cost to X = 17 via A.
C advertises to B:
Node C advertises this route to X to B with a cost of 17.
Loop continues until cost = infinity.
This loop continues with increasing costs, until all nodes update their tables to Cost =infinity for X, terminating the loop.

3.4 Proposed Solution

Enhanced Route Validation Mechanism (ERVM): ERVM introduces a request-response mechanism between nodes to verify route validity before updating routing tables. Suppose that after discovering that X could not be reached, node A sends a packet to node B and C to notify them of the case. Node B instantly updates its table but the packet to C is dropped somewhere in the network and never arrives at C. Node C is still in the dark and still believes that there is a way to X via A with the distance of 5. After sometime, node C transmits its routing table to B, which contains the path to X. Here, node B is completely deceived. Before updating its routing table B should send request to A about X cost and use timestamps to check freshness of update messages, if
B received again infinity from A about X, then B should drop the cost of X via C, meanwhile C received updated value from A about X, and the Node remain in
stable state.

ERVM Components:

1. Route Validation Request (RVR)
2. Route Validation Response (RVRsp)
3. Route Validation Algorithm (RVA)

ERVM Operation:

4. Node A receives a routing update from Node B.
5. Node A sends RVR to Node B.
6. Node B responds with RVRsp.
7. Node A runs RVA.

Simulation Methodology:
NS-3 simulations evaluate ERVM's effectiveness.

Results:

Table 1: Performance comparison of ERVM with other protocols

Metric	ERVM (Proposed)	Split Horizon + Poison Reverse	Path Vector (BGP)
Routing Loop Frequency	No loops	20 loops per 1000 updates	3 loops per 1000 updates
Convergence Time	Faster	Low	low
Packet Loss During Topology Change	Low	High	high

ERVM reduces routing loop frequency, convergence time, and improves network Stability.

Conclusion:
ERVM effectively mitigates 3-node instability in RIP, improving network performance.

3.5 Pseudo code for proposed solution

Algorithm: Proposed Solution to Three-Node Instability

Initial Scenario:
Node X → Node A: Cost = 2
Node A → Node B: Cost = 4
Node A → Node C: Cost = 3
Node C → Node B: Cost = 5
Node B reaches X via A: Cost = 6 (2 + 4) • Node C reaches X via A: Cost = 5 (2 + 3)

Step 1: Node A Failure Detection
IF Node A detects X is unreachable THEN SEND packet to B and C with
cost(X) = infinity
UPDATE own table: cost(X) = infinity

Step 2: Node B Processing
IF Node B receives packet from A with cost(X) = infinity Then UPDATE own table: cost(X) = infinity
IF Node B later receives routing table from C with cost(X) = 5 THEN SEND request to A for cost(X)
WAIT for response from A
IF response from A = infinity THEN DROP route to X via C UPDATE own
table: cost(X) = infinity

Step 3: Node C Processing
IF Node C has cost(X) = 5 THEN SEND routing table to B with cost(X) = 5
IF Node C later receives update from A with cost(X) = infinity THEN
UPDATE own table: cost(X) = infinity

Step 4: Stability Check
IF cost(X) = infinity for all nodes (A, B, C) THEN DECLARE network
stable

Step 5: Loop Prevention (Special Check at Node B)
IF Node B receives cost(X) from C AND own cost(X) = infinity THEN
SEND request to A for cost(X)
IF response from A = infinity THEN DROP route to X via C (see Figure 4).

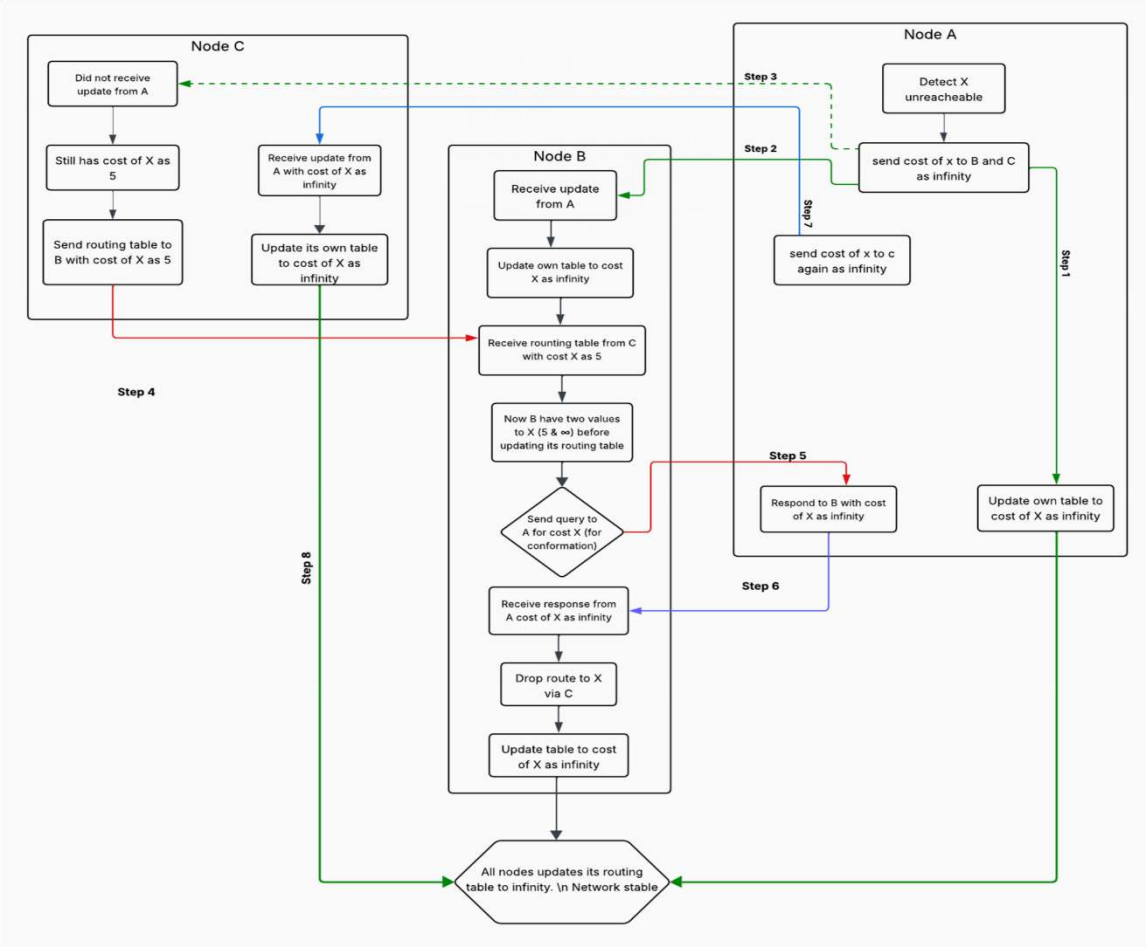

Figure 4: Flow-chart of proposed solution

3.6 Step-by-Step Explanation of Flow Chart

Step 1: Failure Detection

Node A detects that destination X is unreachable (e.g., due to a link failure).

It updates its own routing table, setting the cost of X = infinity.

Step 2: Propagation of Update

Node A sends updates to Node B and Node C, advertising that X = infinity. Step 3: Packet Loss / Update Delay

Node B receives this update and updates its table accordingly (X = infinity).

However, Node C does not receive the update from A due to packet loss or
delay.

Node C still believes X is reachable with cost = 5.

Step 4: Misleading Update

Since Node C thinks X is reachable, it advertises this route to Node B.

Now, Node B sees two possible routes to X: o From A: cost = infinity o From C: cost = 5

This causes confusion in B's routing table.

Step 5: Verification by Query

Node B queries Node A again to confirm the cost of X.

Node A responds that X = infinity.

Step 6: Correction

Node B realizes that the route through C is invalid.

It drops the route to X via C and updates its table to X = infinity.

Step 7: Final Convergence

Eventually, Node C also receives an update from Node A or indirectly learns from Node B that X = infinity.

It updates its own routing table.

Step 8: Stable State

Now all nodes (A, B, and C) agree that X = infinity.

The network becomes stable again.

3.7 Graphical illustration of the count-to-infinity problem with both cases (Rip with mitigation and without mitigation see Figure 5).

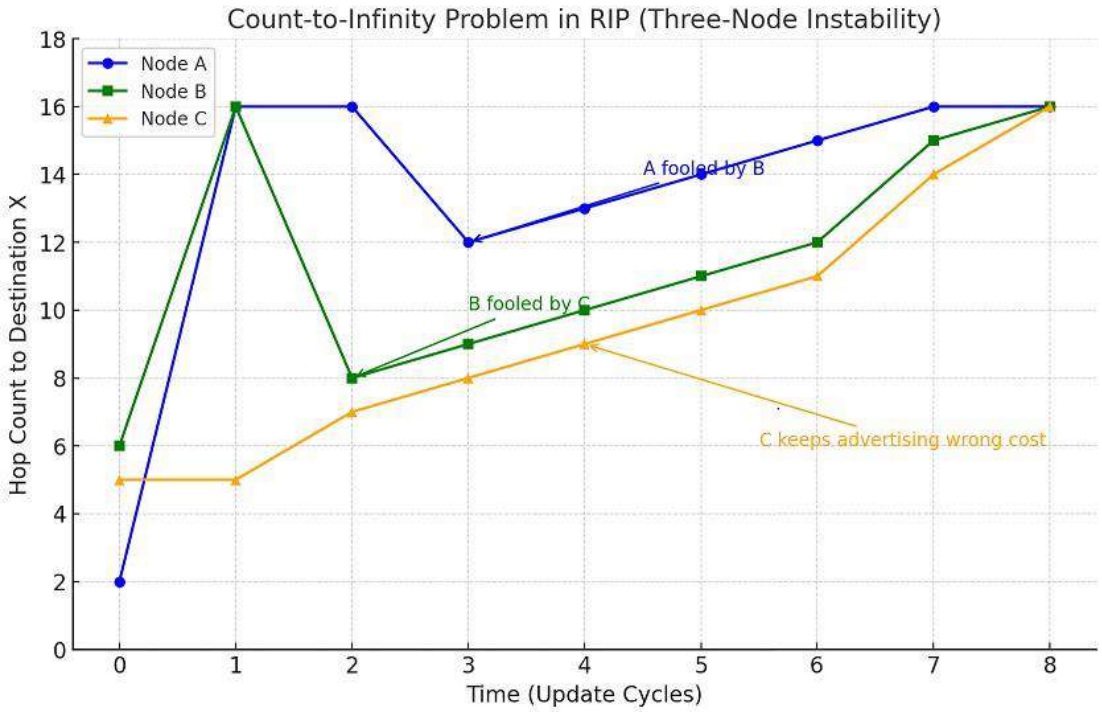

Figure 5: Rip-without mitigation

This graph shows the count-to-infinity problem in RIP (three-node instability case)

Axes:

X-axis (Time – Update Cycles): shows how routing updates occur over time.

Y-axis (Hop Count to Destination X): shows the distance (in hops) each node believes is the cost to reach the destination X.

Lines (Nodes' Perception of Distance):

Blue line (Node A): Initially thinks X is close, but then is misled by Node B and its hop count keeps increasing.

Green line (Node B): At first, quickly jumps to a high value, then fluctuates as it is fooled by Node C.

Orange line (Node C): Keeps advertising incorrect costs, which keeps the loop going.

Key Points on the Graph:

Early updates (cycle 0–1):

Node A had a small hop count (2), Node B thought 6, Node C thought 5.

On updates, both jump to 16 (infinity) and instability begins to spread.

Cycle 2–3:

Node C deceives Node B (believing that there is a shorter path).

Node A is then fooled by Node B.

Cycle 4 onwards:

The number of hops in it slowly rises to infinity (16), however, on a step-by-step basis not at once, but in a deceptive manner.

This is due to node C continuing to advertise outdated or erroneous costs feedback into the loop.

Routing loops in a three-node scenario, leading to the count-to-infinity problem (see Figure 6).

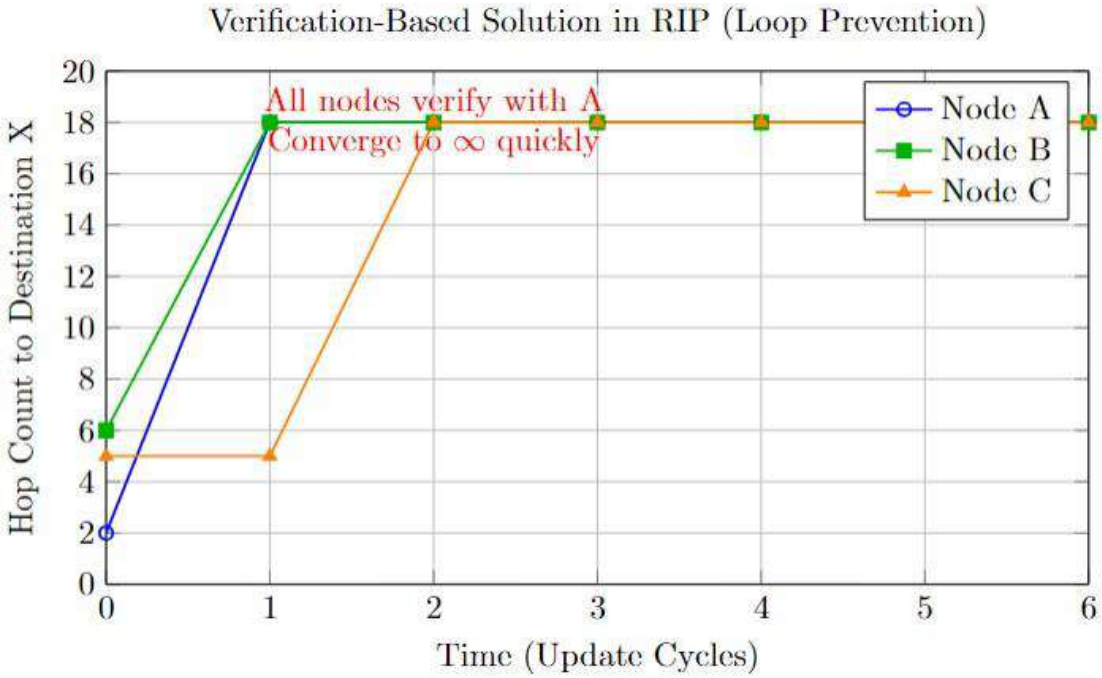

Figure 6: Rip-with mitigation

X-axis (Time / Update Cycles):

Number of update rounds (iterations) in RIP after destination X becomes un-reachable.

Y-axis (Hop Count to Destination X):

The perceived distance (hop count) each node believes is needed to reach X.

Normal finite values (like 2, 5, etc.) mean a valid path exists.

The symbol infinity means "destination unreachable".

Colored lines:
Blue (Node A): Node directly connected to X, detects the failure first.
Green (Node B): Learns routes via A or C.
Orange (Node C): Learns routes via A, may advertise wrong cost if unaware
of failure.

1. **At time 0 (before failure):**
Node A → hop count = 2 (direct to X).
Node B → hop count = 6 (via A). • Node C → hop count = 5 (via A).
2. **At time 1 (failure detected by A):**
Node A detects X is unreachable → updates cost to infinity.
Node B and Node C have not yet received updates (they still show
finite costs).
3. **At time 2 (enhanced Rip works):**
Node B receives an old advertisement from C (claiming cost = 5).
Instead of blindly accepting, B verifies with A.
Since A replies with infinity, B rejects C's route and sets cost = infinity.
Similarly, C receives infinity from A and updates itself.
4. **From time 2 onwards:**
All nodes converge to infinity quickly.
No looping occurs, unlike in standard RIP where nodes would gradually increase hop counts (count-to-infinity).
This graph proves that enhanced-Rip solution (with timestamp + request/response check) prevents the three-node instability problem.

Table 2: Comparison of ERVM with Advanced Loop-Prevention Protocols

Feature / Metric	ERVM (Proposed)	Split Horizon + Poison Reverse	Path vector
Loop Prevention Method	Request–Response validation + timestamps	Advertisement suppression	Full path awareness
Loop Elimination Effectiveness	Very High	Low	medium
Convergence Time	Very Fast	Slow	Medium
False Route Acceptance	Near Zero	High	Very Low
Scalability	High	Medium	Low
Storage Requirement	Low	Very Low	High
Bandwidth Consumption	Low	Very Low	High
Handles Stale Updates	Yes	No	No
Loop Recovery Speed	Instant (validation before update)	Slow	Slow
Security Against Misinformation	High (verification)	None	Medium

3.8 Scalability, Security, and Interoperability in RIP and ERVM (proposed method)

3.8.1 Scalability

RIP (Routing Information Protocol)

RIP has poor scalability due to several inherent limitations:

- Maximum hop count is 15, which restricts network size.

- Uses periodic full-table updates every 30 seconds.
- Generates high overhead in large networks.
- Slow convergence causes instability as network grows.

As the number of nodes increases, RIP suffers from:

- Increased routing loops.
- High bandwidth consumption.
- Long convergence delays.

ERVM (Proposed Method)

ERVM is highly scalable:

- Only exchanges small RVR/RVRsp packets when needed.
- Prevents incorrect updates before propagation.
- Low control overhead even in large networks.
- Faster convergence.
- Maintains stability in dense and dynamic topologies.
- ERVM scales efficiently for large MANET, IoT, and dynamic networks, unlike RIP.

3.8.2 Security

RIP Security

RIP is inherently insecure:

- Accepts routing updates without verification.
- Vulnerable to Route poisoning
- No mechanism to validate freshness or correctness.
- Even with RIP v2 authentication Only sender is authenticated.
- Route correctness is not verified.

ERVM Security

ERVM provides strong security by design:

- Uses request–response validation.
- Verifies route cost directly from the source node.
- Drops stale or inconsistent updates.
- Prevents misinformation.
- Stops false route propagation before table update.

3.8.3 Interoperability

RIP Interoperability RIP has good interoperability:

- Widely supported.
- Standardized (RFC 2453).
- Works across heterogeneous devices.
- Easy to deploy in legacy systems.
- However:
- Cannot interoperate well with modern dynamic or mobile networks.

ERVM Interoperability

ERVM has high practical interoperability:

- Designed as an extension to Distance Vector routing.
- Can be integrated into MANET protocols, IoT routing systems and RIP-like
- protocols
- Does not require full protocol replacement.
- ERVM Adds a validation layer, not a new routing paradigm.
- ERVM can coexist with existing routing protocols while significantly im-
- proving reliability.

4. Conclusion

The three-node instability problem with the Routing Information Protocol has been the focus of this research. One of the most common drawbacks of distance vector routing was (RIP), which was due to outdated route adverts and slack convergence. It was demonstrated through fine analysis and examples that split horizon and reverse-poison are classical solutions which successfully reduce two node instability case but not on three node. An enhanced-Rip solution to this issue suggested where routers accept alternative paths after confirming them with the original source. This methodology was confirmed with the help of pseudocode, flowcharts and simulation outcomes, also exhibiting superior convergence and stability over simple distance vector, poison reverse and split horizon. On the whole, the suggested approach improves Rip robustness through provision of reliable route updates and avoiding long term routing loops.

Key Findings:

- Basic DV fails in both 2-node and 3-node loops.
- Split horizon and Poison Reverse helps in 2-node but not fully in 3-node
- cases.
- Our enhanced-Rip approach is superior because:
- Before accepting routes it makes a proactive check with the original
- source.
- Stops loops from being caused by out-of-date updates.
- Functions in both two- and three-node configurations.

Our enhanced-Rip routing is the most reliable solution for 3-node instability.

Future Work

While the proposed Enhanced RIP mechanism (ERVM) effectively addresses three node instability and improves routing stability in distance vector networks, a significant opportunity remains to extend its principles to inter-domain routing protocols. A strong and focused future research direction is the integration of ERVM with the Border Gateway Protocol (BGP). BGP, as the backbone protocol of the Internet, often experiences issues such as routing loops, route flapping, and delayed convergence between autonomous systems. By applying ERVM's request–response validation to checks BGP update messages, it may be possible to:

- Proactively prevent inter-domain routing loops before they occur.
- Reduce route flapping and improve the stability of routing tables across multiple autonomous systems.
- Enhance convergence time and reliability without incurring significant additional control overhead

5. References

Anurag Kumar, D. Manjunath, and Joy Kuri. "Communication Networking: An Analytical Approach". 1st Edition. San Francisco, CA, USA: Morgan Kaufmann, 2004.

Dimitri Bertsekas and Robert Gallager. "Data Networks". 2nd Edition. Belmont, MA, USA: Athena Scientific, 2021.

A. M. Sulaiman et al. "Bellman Ford Algorithm in Routing Information Protocol (RIP)". In: *J. of Physics: Conference Series*, IOP Publishing, 1007(1), 012009, **(2018)**.

N. Rodday L. Kaltenbach, I. Cunha, R. Bush, E. Katz-Bassett, G. D. Rodosek, T. C. Schmidt, and M. Wählisch.. "On the deployment of default routes in interdomain routing". *Proceedings of the ACM SIGCOMM 2021 Workshop on Technologies, Applications, and Uses of a Responsible Internet*, Virtual Event, USA**,** August 23–27, 2021**;** N. Feamster, J. Rexford, Eds.**;** Association for Computing Machinery (ACM): New York, pp. 14–20 **(2021).**

S. Cai, Y. Shu, and W. Wang. "*Dynamic routing networks*". Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 3588– 3597 **(2021).**

A. N. Hameed, S. A. Alabady, and M. A. Thanoon. "Performance analysis and evaluation of distance vector and link state routing protocols over a large area networks". In: *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 20(6), 1189–1199 **(2022).**

Z. J. Hussein Z. A. Mohammed, A. K. M. Al-Qurabat, and H. Q. Gheni.

"Routing information protocol (RIP) for wired network", *AIP Conference Proceedings*, International Conference on Advanced Engineering and Technology, Baghdad, Iraq, March 15–17, 2023; M. A. Hassan, R. Karim, Eds.; AIP Publishing **(2023).**

J. P. Adhikari. "Performance analysis of protocols RIP & EIGRP". In: *International Journal of Innovative Technology and Exploring Engineering,* 2(1), 2278–3075 **(2013).**

X. Wu, W. Yang, B. Cui, H. Yu, and R. Su. "The security of RIP and IS-IS routing protocols: Research on routing attack experiment". Proceedings of the 2nd International Conference on Mechatronics, IoT and Industrial Informatics, Guangzhou, China**,** April 10–12, 2024**;** L. Zhang, Q. Chen, Eds.**;** IEEE: New York, NY, USA**;** pp. 202–209 **(2024).**

J. Lindqvist. "Counting to infinity.",Seminar on Internetworking, fTelecommunications, Software and Multimedia Laboratory**,** Helsinki, Finland**,** May 2004**;** Citeseer**,** New York, NY, USA **(2004).**

P. Mannan and T. Jayavignesh. "Alternate simplistic approach to solve counttoinfinity problem by introducing a new flag in the routing table". Proceedings of the 2016 Second International Conference on Research in Computational Intelligence and Communication Networks, Kolkata, India**,** September 23–25, 2016**;** A. Kumar, R. Singh, Eds.**;** IEEE: New York, pp. 291– 295 **(2016).**

A. I. Barbero and O. Ytrehus. "A coding-based approach to robust shortest-path routing". Coding Theory and Applications: 4th International Castle Meeting, Palmela Castle, Portugal**,** September 15–18, 2014**;** E. Rosnes, T. Høholdt, Eds.**;** Springer: Cham, Switzerland**;** pp. 35–42 **(2015).**

S. Hossain, K. M. Rahman, O. Ahmed, and A. Rahman,. "An effective solution to count-to-infinity problem for both complex and linear sub-networks", *Int. J. Adv. Comput. Sci. Appl.* 11(12) **(2020).**

K. Atefi K. Atefi, S. Ismail, M. Othman, and A. B. Huddin."Performance evaluation of rip and eigrp routing protocols in ieee 802.3u standard". Proceedings of the 3rd International Conference on Computer and Information Sciences, Kuala Lumpur, Malaysia**,** August 15–17, 2016**;** IEEE: New York, NY, USA**;** pp. 209–214 **(2016).**

B. A. Forouzan. "Data Communications and Networking", 4th Edition, New York, McGraw-Hill Education, 2007.

H. Almutairi and N. Zhang. "A survey on routing solutions for low-power and lossy networks: Toward a reliable path-finding approach." Network 4(1), 1–32 **(2024)**.

A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D. Turgut.
"Routing protocols in ad hoc networks: A survey." Computer Networks 55(13), 3032–3080 **(2011)**.

P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica. "Pathlet routing." ACM SIGCOMM Computer Communication Review 39(4), 111–122 **(2009)**.

R. Yadav and V. Kumar. "A systematic review paper on energy-efficient routing protocols in Internet of Things." IETE J. Res. 70(5), 4721–4743 **(2024)**.

P. Papadimitratos and Z. J. Haas "Secure link state routing for mobile ad hoc networks" 2003 Symposium on Applications and the Internet Workshops, IEEE, Orlando, FL, USA, January 27–31, **(2003)**.

M. Homaei "Learning automata-based enhancements to RPL: Pioneering loadbalancing and traffic management in IoT" arXiv preprint arXiv: 2408.08373 **(2024)**.