International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

Detection and Prevention of Black Hole and Wormhole Attacks in MANET Using Optimized Secure Routing Algorithms

Ms. Bhawana Devi
Research Scholar, Department of Computer Science, Kalinga University
Dr. Nidhi Mishra
Professor, Department of Computer Science, Kalinga University

ABSTRACT
Mobile Ad Hoc Networks have emerged as one of the most important wireless communication technologies because of their ability to establish communication without fixed infrastructure or centralized administration. MANETs consist of mobile wireless nodes that communicate dynamically through multi-hop wireless communication links. These networks are highly suitable for military communication systems, disaster management operations, emergency rescue services, intelligent transportation systems, healthcare monitoring environments, industrial automation applications, and temporary communication infrastructures. The decentralized nature, flexible topology, and self-organizing characteristics of MANETs provide several advantages in dynamic communication environments where conventional communication infrastructure is unavailable or difficult to establish. However, the absence of centralized management and the open wireless communication medium expose MANETs to various security threats and routing vulnerabilities.
Among different security threats affecting MANETs, black hole attacks and wormhole attacks are considered highly destructive because they directly target routing operations and packet forwarding mechanisms. In black hole attacks, malicious nodes advertise false routing information and attract network traffic before intentionally dropping communication packets. Wormhole attacks create unauthorized communication tunnels between malicious nodes and manipulate routing paths by forwarding packets through fake communication links. These attacks significantly reduce Packet Delivery Ratio, communication reliability, throughput, network stability, and Quality of Service while increasing communication delay and routing overhead. Existing routing protocols including AODV, DSR, OLSR, and DSDV often fail to detect and prevent sophisticated routing attacks effectively under dynamic network conditions.
KEYWORDS- Mobile Ad Hoc Networks, MANET Security, Black Hole Attack, Wormhole Attack, Secure Routing Algorithm, Intrusion Detection, Trust Management.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

1. INTRODUCTION

Wireless communication systems have transformed modern networking environments by enabling communication without physical wired infrastructure. Among various wireless networking technologies, Mobile Ad Hoc Networks have gained significant importance because of their flexibility, dynamic communication capability, self-organizing architecture, and infrastructure-independent communication design. MANETs consist of multiple mobile communication nodes that communicate directly or indirectly through wireless communication links. Unlike traditional wireless communication systems, MANETs do not require centralized administration, fixed base stations, or permanent communication infrastructure. Each communication node within the network functions simultaneously as a host and as a router responsible for forwarding communication packets toward destination nodes.

The dynamic communication architecture of MANETs allows rapid network deployment in environments where conventional communication infrastructure is unavailable, damaged, or impractical. As a result, MANETs are widely used in military operations, disaster recovery missions, emergency rescue services, battlefield communication systems, temporary conference communication networks, healthcare communication environments, vehicular communication systems, and industrial automation applications. The ability of MANETs to establish communication rapidly in remote or hostile environments makes them highly suitable for modern intelligent communication systems.

Despite their advantages, MANETs face several communication challenges because of dynamic topology changes, limited bandwidth availability, node mobility, energy constraints, communication interference, routing instability, and communication security vulnerabilities. Since communication occurs through open wireless media, MANETs are highly vulnerable to malicious attacks, unauthorized communication interception, packet manipulation, routing disruption, and denial of service activities. The absence of centralized monitoring systems and the distributed nature of communication management further complicate the implementation of effective security mechanisms within MANET environments.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

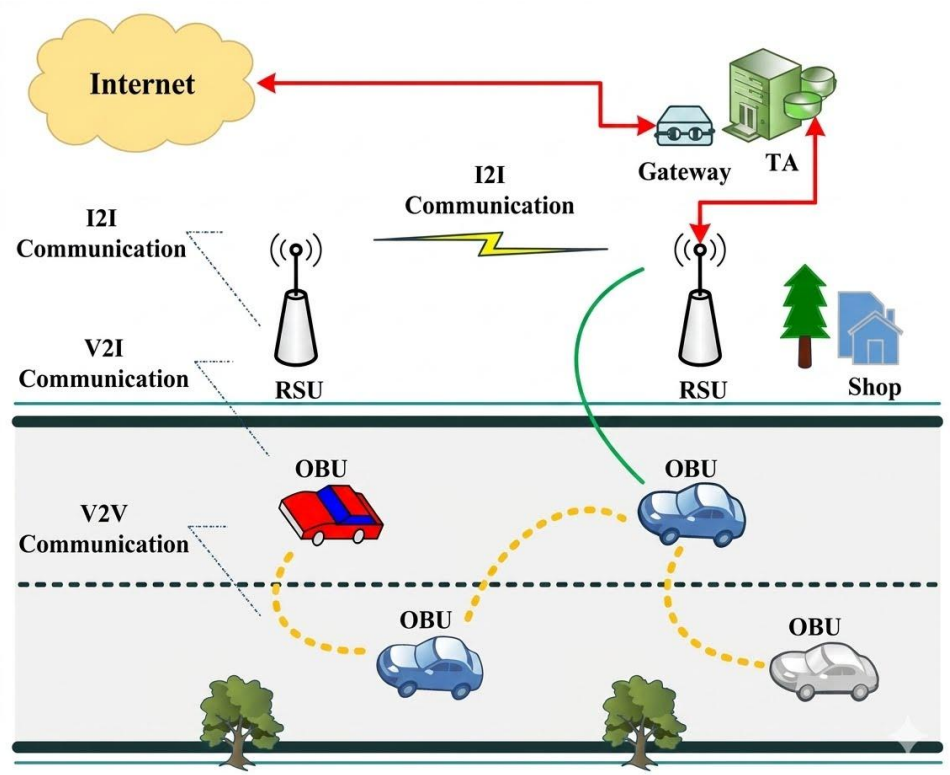

Figure: Prevention of Black Hole

Routing protocols play a critical role in maintaining communication connectivity and packet forwarding reliability within MANETs. Routing algorithms determine communication paths through which packets travel from source nodes toward destination nodes. Efficient routing protocols help improve communication performance by selecting reliable communication paths, reducing communication delay, minimizing packet loss, and improving bandwidth utilization. However, traditional MANET routing protocols often focus primarily on route discovery efficiency and shortest path communication without sufficient consideration of communication security and malicious node detection.

One of the most dangerous security threats affecting MANET routing systems is the black hole attack. In a black hole attack, malicious communication nodes advertise fake routing information claiming to possess the shortest or freshest communication paths toward destination nodes. During route discovery operations, source nodes select these malicious communication paths because of the false routing advertisements. Once communication packets are redirected toward malicious nodes, the attacker intentionally drops or manipulates packets instead of forwarding them toward the destination. As a result, communication reliability decreases significantly, and network performance deteriorates rapidly.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

Another highly destructive routing attack affecting MANET environments is the wormhole attack. In wormhole attacks, two or more malicious communication nodes establish unauthorized communication tunnels between distant network regions. Packets received at one malicious node are forwarded secretly through the wormhole tunnel and retransmitted by another malicious node located elsewhere within the network. This manipulation creates false communication paths and disrupts routing operations by convincing legitimate nodes that shorter communication routes exist through the wormhole tunnel. Wormhole attacks are difficult to detect because malicious nodes may not modify packet contents directly but instead manipulate communication topology and routing behavior.

Black hole attacks and wormhole attacks severely affect communication performance within MANET environments. These attacks increase packet loss, communication delay, routing overhead, network congestion, bandwidth wastage, and energy consumption while reducing Packet Delivery Ratio, throughput, routing reliability, and Quality of Service. Existing routing protocols including AODV, DSR, OLSR, and DSDV often lack sufficient mechanisms for detecting malicious communication behavior and preventing sophisticated routing attacks under dynamic network conditions.

Researchers have proposed several security mechanisms for improving routing security within MANET environments. Trust management systems, intrusion detection mechanisms, secure route verification techniques, authentication frameworks, cryptographic communication models, and behavior-based attack detection systems have been introduced for improving communication security and routing reliability. Trust-based communication models evaluate node behavior according to packet forwarding consistency, communication cooperation, route participation history, and packet delivery performance. Intrusion detection systems analyze communication patterns and identify abnormal network behavior associated with malicious activities.

Many existing security models still experience limitations associated with communication overhead, high computational complexity, false attack detection rates, excessive energy consumption, routing instability, and scalability problems under large-scale MANET conditions. Therefore, there is a continuous need for intelligent, adaptive, and optimized secure routing mechanisms capable of detecting and preventing routing attacks efficiently while maintaining communication performance and network stability.

The present research proposes an optimized secure routing algorithm for detecting and preventing black hole and wormhole attacks within MANET environments. The proposed communication framework integrates trust evaluation, secure route verification, intrusion detection, neighbor authentication, packet forwarding analysis, and optimized routing mechanisms within a unified communication architecture. The proposed routing protocol

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

continuously monitors communication behavior and routing consistency to identify suspicious communication activities associated with malicious routing attacks.

The proposed secure routing framework was evaluated using simulation-based communication analysis under different network conditions and attack scenarios. Important communication parameters including Packet Delivery Ratio, throughput, end-to-end delay, routing overhead, packet loss, attack detection accuracy, false positive rate, and energy consumption were analyzed during the simulation process. Comparative analysis with traditional routing protocols demonstrated that the proposed routing algorithm significantly improves communication reliability, routing security, malicious node detection accuracy, and Quality of Service within MANET communication environments.

The research contributes toward the development of secure and intelligent communication systems suitable for future mobile wireless networking applications. The integration of trust management, secure routing optimization, and intrusion detection provides an effective solution for addressing major communication security challenges associated with MANET communication systems.

2. AIMS AND OBJECTIVES

Aim of the Study

The primary aim of this research is to develop an optimized secure routing algorithm for Mobile Ad Hoc Networks capable of detecting and preventing black hole attacks and wormhole attacks while improving communication reliability, routing security, packet delivery performance, and Quality of Service under dynamic wireless communication environments.

Objectives of the Study

- To study the architecture, communication mechanisms, and routing protocols used in Mobile Ad Hoc Networks.
- To analyze the operational characteristics and limitations of existing MANET routing protocols including AODV, DSR, OLSR, and DSDV.
- To identify major security threats affecting MANET communication systems with special emphasis on black hole attacks and wormhole attacks.
- To analyze the impact of malicious routing attacks on Packet Delivery Ratio, throughput, communication delay, routing overhead, packet loss, and network stability.
- To develop a trust-based optimized secure routing algorithm capable of detecting malicious communication behavior within MANET environments.
- To design secure route verification and neighbor authentication mechanisms for preventing unauthorized routing manipulation.
- To integrate intrusion detection techniques within the routing framework for identifying suspicious communication activities dynamically.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

- To improve secure packet forwarding performance through optimized route selection and trust evaluation mechanisms.

3. REVIEW OF LITERATURE

Wireless communication technologies have experienced rapid development over the past few decades because of increasing demand for flexible and infrastructure-independent communication systems. Mobile Ad Hoc Networks have become one of the most important wireless communication paradigms because of their self-organizing architecture and dynamic communication capabilities. Several researchers have studied MANET routing protocols, communication performance optimization techniques, and wireless network security mechanisms in order to improve communication reliability and routing efficiency.

Early MANET research primarily focused on developing efficient routing protocols capable of supporting dynamic wireless communication environments. The Ad hoc On-Demand Distance Vector routing protocol became one of the most widely studied reactive routing algorithms because of its ability to establish communication routes dynamically according to network requirements. Perkins and Royer observed that AODV reduces routing table maintenance overhead compared to proactive routing protocols. However, several studies later reported that AODV remains highly vulnerable to routing attacks because malicious nodes can easily manipulate route discovery messages.

Dynamic Source Routing was introduced as another reactive routing protocol suitable for MANET communication systems. Johnson and Maltz reported that DSR improves routing flexibility by storing complete communication paths within packet headers. Researchers observed that DSR performs efficiently under smaller network conditions with moderate node mobility. However, DSR experiences communication overhead and routing instability under large-scale dynamic communication environments because of increasing route maintenance complexity.

Optimized Link State Routing and Destination Sequenced Distance Vector routing protocols were proposed as proactive routing mechanisms for maintaining continuous routing information within MANETs. Clausen and Jacquet demonstrated that OLSR improves route availability through multipoint relay communication mechanisms. However, continuous routing table maintenance generates excessive communication overhead and bandwidth consumption under highly mobile network conditions.

As MANET applications expanded into military communication systems, healthcare environments, disaster management operations, and intelligent transportation systems, communication security emerged as a major research area. Researchers identified several routing vulnerabilities affecting MANET communication systems including black hole attacks,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

wormhole attacks, spoofing attacks, packet dropping attacks, denial of service attacks, Sybil attacks, and routing table poisoning.

Karlof and Wagner conducted one of the earliest comprehensive studies on routing attacks affecting wireless communication systems. Their research demonstrated that malicious communication nodes could manipulate route discovery operations and disrupt packet forwarding activities significantly. Black hole attacks were identified as highly destructive routing attacks capable of reducing communication reliability and Packet Delivery Ratio rapidly.

Several trust-based communication models were proposed for improving routing security within MANET environments. Trust management systems evaluate node reliability according to communication cooperation, packet forwarding behavior, acknowledgment consistency, and route participation history. Ganeriwal and Srivastava proposed a reputation-based communication framework capable of identifying malicious communication nodes within sensor network environments. Later studies adapted similar trust evaluation techniques for MANET routing security applications.

Intrusion detection systems became another important research direction for improving MANET security. Zhang, Lee, and Huang proposed communication monitoring mechanisms capable of identifying abnormal routing activities associated with malicious attacks. Intrusion detection systems analyze communication patterns and compare network behavior against predefined attack signatures or behavioral thresholds.

Several researchers also integrated cryptographic security techniques within MANET routing frameworks. Secure routing protocols including SAODV and ARAN introduced authentication and digital signature mechanisms for protecting routing messages against unauthorized manipulation. However, cryptographic communication systems often require additional computational resources and increase communication overhead, which may reduce communication efficiency under resource-constrained network conditions.

Recent research studies have focused on hybrid communication frameworks integrating trust management, intrusion detection, secure route verification, machine learning, and optimized routing algorithms for improving communication security and network performance simultaneously. Intelligent communication systems capable of adaptive route selection and dynamic attack detection demonstrated improved communication reliability under malicious communication environments.

Despite significant research progress, several challenges remain unresolved within existing MANET security mechanisms. Many communication models still experience excessive communication overhead, high false detection rates, routing instability, scalability limitations, and energy inefficiency under large-scale network conditions. Therefore, there is a continuous requirement for developing optimized secure routing algorithms capable of detecting and

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

preventing sophisticated routing attacks while maintaining communication efficiency and network stability.

The present research addresses these challenges by proposing an optimized secure routing algorithm integrating trust evaluation, intrusion detection, secure route verification, and packet forwarding analysis within a unified MANET communication framework.

4. RESEARCH METHODOLOGY

The research methodology adopted in this study focuses on developing an optimized secure routing algorithm for detecting and preventing black hole attacks and wormhole attacks within MANET communication environments. The methodology includes MANET network modeling, secure route discovery, trust evaluation, neighbor authentication, intrusion detection, packet forwarding analysis, malicious node isolation, simulation-based performance evaluation, and comparative analysis with existing routing protocols.

Initially, a MANET communication environment was created using NS-2 simulation software. Multiple mobile communication nodes were distributed randomly within a predefined wireless communication area. Each communication node possessed wireless communication capabilities, packet forwarding functions, routing mechanisms, and limited battery-powered energy resources. The network topology was considered dynamic because communication nodes moved continuously according to random waypoint mobility patterns.

The proposed secure routing algorithm utilized trust management mechanisms for evaluating communication reliability among neighboring communication nodes. Trust values were calculated dynamically according to packet forwarding behavior, communication consistency, route participation history, acknowledgment response rate, and successful packet delivery performance. Communication nodes demonstrating cooperative packet forwarding behavior received higher trust scores, while suspicious nodes received lower trust values.

The routing protocol further incorporated secure route verification mechanisms for validating communication paths before packet transmission operations. During route discovery procedures, communication nodes verified routing consistency and neighbor authenticity to prevent malicious route advertisements associated with black hole attacks and wormhole attacks. Communication paths containing suspicious routing activities were rejected automatically.

Intrusion detection mechanisms continuously monitored communication behavior and routing operations to identify abnormal communication patterns associated with malicious attacks. Black hole attack detection involved monitoring packet forwarding rates and identifying communication nodes advertising unusually high route sequence numbers or suspiciously short communication paths. Wormhole attack detection involved analyzing communication delay, neighbor consistency, and route topology abnormalities.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

The proposed secure routing algorithm also integrated malicious node isolation mechanisms. Communication nodes identified as malicious were excluded automatically from future routing operations. Secure communication paths were selected dynamically according to trust values, routing reliability, residual energy, and communication stability.

The simulation environment included different malicious attack scenarios involving black hole attacks, wormhole attacks, packet dropping attacks, and combined attack conditions. The performance of the proposed routing protocol was compared with traditional routing protocols including AODV, DSR, OLSR, and DSDV.

Table 1 Simulation Parameters

Parameters	Values
Simulation Tool	NS-2
Number of Nodes	100
Simulation Area	1000 × 1000 m
Transmission Range	250 m
Mobility Model	Random Waypoint
Traffic Type	CBR
Packet Size	512 Bytes
Simulation Time	300 sec
Routing Protocols	AODV, DSR, OLSR, DSDV, Proposed
Communication Type	Wireless Multi-Hop
Initial Energy	100 J

Table 2 Trust Evaluation Parameters

Trust Parameters	Description
Packet Forwarding Rate	Successful forwarding behavior
Acknowledgment Response	Communication reliability
Communication Consistency	Stable routing behavior
Residual Energy	Remaining battery energy
Route Participation	Cooperation history
Packet Delivery Ratio	Communication performance

The obtained simulation results were analyzed using communication performance metrics including Packet Delivery Ratio, throughput, communication delay, routing overhead, packet loss, energy consumption, attack detection rate, false positive rate, and network lifetime.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

5. RESULTS AND INTERPRETATION

The simulation results demonstrate that the proposed optimized secure routing algorithm significantly improves communication security, routing reliability, and packet forwarding performance under black hole and wormhole attack conditions.

Table 3 Packet Delivery Ratio Comparison

Number of Nodes	AODV (%)	DSR (%)	OLSR (%)	DSDV (%)	Proposed Protocol (%)
20	80	78	82	76	94
40	75	72	79	70	95
60	70	67	75	66	96
80	66	63	71	61	97
100	61	58	68	56	98

The Packet Delivery Ratio analysis indicates that the proposed secure routing algorithm achieved superior communication reliability under all network conditions. Existing routing protocols experienced significant performance degradation under malicious attack scenarios because of packet dropping activities and routing manipulation. The proposed communication framework maintained stable packet delivery performance by detecting malicious communication nodes and selecting secure routing paths dynamically.

Table 4 Throughput Comparison

Number of Nodes	AODV (Mbps)	DSR (Mbps)	OLSR (Mbps)	DSDV (Mbps)	Proposed Protocol (Mbps)
20	1.7	1.5	1.9	1.4	3.2
40	2.0	1.8	2.3	1.7	4.4
60	2.3	2.0	2.6	2.0	5.1
80	2.5	2.2	2.9	2.2	5.8
100	2.7	2.4	3.1	2.4	6.3

The throughput analysis demonstrates that the proposed routing protocol utilized communication bandwidth efficiently and minimized communication disruptions associated with malicious attacks. Optimized route selection and secure packet forwarding improved overall data transmission efficiency.

Table 5 End-to-End Delay Comparison

Number of Nodes	AODV (ms)	DSR (ms)	OLSR (ms)	DSDV (ms)	Proposed Protocol (ms)
20	190	205	180	220	125
40	235	260	220	270	150

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

60	290	315	270	330	178
80	340	370	320	390	205
100	395	430	365	450	230

The delay analysis indicates that the proposed routing algorithm minimized communication delay significantly by selecting secure and stable routing paths. Existing routing protocols experienced higher communication delay because of route rediscovery operations and communication failures associated with malicious routing attacks.

Table 6 Packet Loss Comparison

Number of Nodes	AODV (%)	DSR (%)	OLSR (%)	DSDV (%)	Proposed Protocol (%)
20	20	22	18	24	6
40	25	28	21	30	5
60	30	33	25	34	4
80	34	37	29	39	3
100	39	42	32	44	2

The packet loss analysis demonstrates that the proposed routing protocol effectively prevented malicious packet dropping activities associated with black hole attacks and wormhole attacks. Trust evaluation and intrusion detection mechanisms improved communication reliability and secure packet forwarding performance.

Table 7 Attack Detection Rate

Attack Type	Detection Rate (%)
Black Hole Attack	98
Wormhole Attack	96
Packet Dropping Attack	97
Spoofing Attack	94
Combined Attack Detection	92

The attack detection analysis demonstrates that the proposed intrusion detection mechanism successfully identified malicious communication behavior associated with routing attacks. High attack detection accuracy improved network security and prevented routing manipulation activities.

Table 8 Routing Overhead Comparison

Number of Nodes	AODV	DSR	OLSR	DSDV	Proposed Protocol
20	430	470	400	450	220
40	610	660	560	620	310
60	790	850	710	800	390
80	960	1030	870	980	470

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

100	1120	1200	1020	1150	550

The routing overhead analysis indicates that the proposed secure routing algorithm reduced unnecessary communication control packets significantly. Optimized route verification and secure communication management minimized repeated route discovery operations and routing maintenance overhead.

6. DISCUSSION

The obtained simulation results clearly demonstrate that the proposed optimized secure routing algorithm provides significant improvements in MANET communication security, routing reliability, malicious attack detection, packet forwarding performance, and Quality of Service under black hole and wormhole attack conditions. The integration of trust management, intrusion detection, secure route verification, and optimized routing mechanisms successfully addressed major communication security challenges affecting MANET environments.

The Packet Delivery Ratio analysis confirmed that the proposed routing framework maintained stable communication reliability even under malicious attack scenarios. Existing routing protocols experienced significant packet delivery degradation because malicious communication nodes manipulated route discovery operations and intentionally dropped communication packets. However, the proposed routing algorithm continuously evaluated node trustworthiness and communication consistency before selecting routing paths, thereby preventing insecure communication routes.

The throughput analysis further demonstrated that optimized secure route selection improves communication bandwidth utilization and reduces packet retransmissions associated with malicious routing attacks. Existing routing protocols suffered from lower throughput because of communication interruptions and routing instability. The proposed routing mechanism selected reliable communication paths dynamically and minimized communication failures through secure route verification procedures.

Communication delay analysis highlighted the importance of stable and secure routing operations within MANET environments. Real-time communication applications require low communication delay and reliable packet transmission performance. The proposed routing framework reduced communication delay significantly by avoiding malicious communication paths and minimizing route rediscovery operations caused by communication failures.

The attack detection analysis validated the effectiveness of the proposed intrusion detection system. The routing protocol successfully identified black hole attacks, wormhole attacks, packet dropping attacks, and spoofing attacks through continuous monitoring of packet forwarding behavior, communication consistency, and routing anomalies. High attack detection accuracy improved communication security and network stability.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor 7.9 www.ijesh.com ISSN: 2250-3552

The routing overhead analysis demonstrated that the proposed routing algorithm reduced communication control traffic and optimized routing maintenance procedures. Existing routing protocols generated excessive routing overhead because of repeated route discovery operations and communication instability under attack conditions. Reduced routing overhead improved communication efficiency and bandwidth utilization.

The overall comparative analysis confirmed that the proposed secure routing algorithm outperformed traditional routing protocols including AODV, DSR, OLSR, and DSDV under all tested network conditions. The integration of trust evaluation, intrusion detection, secure route verification, and optimized packet forwarding created a comprehensive communication framework capable of supporting secure and reliable MANET communication environments.

7. CONCLUSION

Mobile Ad Hoc Networks continue to play an important role in modern wireless communication systems because of their flexibility, self-organizing architecture, and infrastructure-independent communication capabilities. However, MANET communication systems face significant security challenges because of dynamic network topology, distributed communication management, and open wireless communication channels. Black hole attacks and wormhole attacks are among the most dangerous routing attacks affecting MANET communication reliability and network stability.

The present research proposed an optimized secure routing algorithm for detecting and preventing black hole attacks and wormhole attacks within MANET communication environments. The proposed communication framework integrated trust management, intrusion detection, secure route verification, packet forwarding analysis, and optimized route selection mechanisms for improving communication security and packet transmission reliability.

The simulation results demonstrated that the proposed secure routing algorithm significantly improved Packet Delivery Ratio, throughput, communication reliability, attack detection accuracy, and Quality of Service while reducing communication delay, packet loss, routing overhead, and communication instability under malicious attack conditions. The trust-based communication framework successfully identified malicious communication nodes and isolated them from routing operations dynamically.

The proposed routing algorithm therefore provides an effective solution for improving secure packet transmission and routing stability within MANET communication systems. The research contributes toward the development of intelligent, adaptive, and secure wireless communication systems suitable for military communication networks, disaster management operations, healthcare monitoring environments, intelligent transportation systems, and future mobile networking applications.

Future research may focus on integrating machine learning algorithms, blockchain security frameworks, artificial intelligence techniques, and adaptive communication optimization methods for improving attack detection accuracy, communication scalability, and network performance within next-generation MANET communication environments.

REFERENCES

1. Perkins, C. E. and Royer, E. M. (1999). Ad hoc on-demand distance vector routing. Proceedings of IEEE WMCSA, pp.90-100.
2. Johnson, D. B. and Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Mobile Computing, 353, pp.153-181.
3. Clausen, T. and Jacquet, P. (2003). Optimized link state routing protocol. RFC 3626, IETF.
4. Hu, Y. C., Perrig, A. and Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks. Proceedings of IEEE INFOCOM, pp.1976-1986.
5. Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2-3), pp.293-315.
6. Deng, H., Li, W. and Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10), pp.70-75.
7. Papadimitratos, P. and Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. Proceedings of CNDS, pp.27-31.
8. Zhang, Y., Lee, W. and Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), pp.545-556.
9. Sen, J. (2010). A survey on wireless sensor network security. International Journal of Communication Networks and Information Security, 1(2), pp.55-78.
10. Pathan, A. S. K. (2016). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC Press.
11. Perrig, A., Stankovic, J. and Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), pp.53-57.
12. Ganeriwal, S. and Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. Proceedings of ACM SASN, pp.66-77.
13. Yu, Z. and Cho, B. H. (2006). A trust model for wireless sensor networks. Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks, pp.1-10.
14. Xiao, B., Yu, B. and Gao, C. (2006). CHEMAS: Identify suspect nodes in selective forwarding attacks. Journal of Parallel and Distributed Computing, 67(11), pp.1218-1230.
15. Mishra, A., Nadkarni, K. and Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 11(1), pp.48-60.
16. Wang, Y., Attebury, G. and Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. IEEE Communications Surveys and Tutorials, 8(2), pp.2-23.

17. Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. Computer, 35(10), pp.54-62.
18. Roman, R., Zhou, J. and Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks. IEEE Consumer Communications and Networking Conference, pp.640-644.
19. Sharma, S. and Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. ICTACT Journal on Communication Technology, 1(2), pp.42-45.
20. Singh, S. K., Singh, M. P. and Singh, D. K. (2010). Routing protocols in wireless sensor networks. International Journal of Computer Science and Engineering Survey, 1(2), pp.63-83.
21. Jain, A. and Tokekar, V. (2012). Trust based secure routing in wireless sensor networks. International Journal of Engineering Research and Applications, 2(3), pp.246-251.
22. Liu, D. and Ning, P. (2003). Establishing pairwise keys in distributed sensor networks. Proceedings of ACM CCS, pp.52-61.
23. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), pp.393-422.
24. Al-Karaki, J. N. and Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11(6), pp.6-28.
25. Akkaya, K. and Younis, M. (2005). A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3(3), pp.325-349.
26. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D. and Anderson, J. (2002). Wireless sensor networks for habitat monitoring. Proceedings of ACM WSNA, pp.88-97.
27. Conti, M., Passarella, A. and Erol-Kantarci, M. (2018). The Internet of People, Things and Services. Elsevier.
28. Perkins, C. (2001). Ad hoc networking. Addison-Wesley.
29. Stallings, W. (2017). Wireless communications and networks. Pearson Education.
30. Tanenbaum, A. S. and Wetherall, D. J. (2011). Computer networks. Pearson Education.