Ijfans International Journal Of Food And Nutritional Sciences
ISSN PRINT 2319 1775 Online 2320 7876
 Journal UGC CARE Listed (Group-I) Volume 10, Issue 10, 2021

Trust-Aware Secure Routing Protocol for Mobile Ad Hoc Networks

Dr. Bijender Bansal[1], Dr. Monika[2], Prof. Deepak Kumar Goyal[3]
[1]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: bijender.vce@gmail.com
[2]Department of Computer Science and Application, Vaish Mahila Mahavidyalaya, Rohtak, Haryana, India Email: monikagoyal.vmm@gmail.com
[3]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: deepakgoyal.vce@gmail.com

Abstract

Mobile Ad Hoc Networks (MANETs) have emerged as a flexible and infrastructure-independent communication technology capable of supporting military operations, disaster recovery, emergency response, intelligent transportation, healthcare monitoring, and mobile computing applications. Despite their advantages, the absence of centralized administration, dynamic topology changes, limited bandwidth, and node mobility expose MANETs to numerous routing attacks such as black hole, gray hole, wormhole, Sybil, and packet dropping attacks. Traditional secure routing protocols primarily rely on cryptographic mechanisms that effectively defend against external attacks but often fail to identify malicious or selfish nodes operating within the network. Trust management has therefore become an effective approach for enhancing routing security by evaluating node behavior during packet forwarding and route discovery. This experimental study proposes a Trust-Aware Secure Routing Protocol (TASRP) for Mobile Ad Hoc Networks that integrates trust evaluation, secure route discovery, authentication, node behavior monitoring, malicious node isolation, and routing performance evaluation into a unified computational framework. The proposed framework combines direct trust, indirect trust, route reliability, and communication efficiency to establish secure and trustworthy communication paths while minimizing routing overhead and packet loss. A mathematical framework and algorithmic strategy are developed to evaluate trust computation, packet delivery ratio, routing overhead, end-to-end delay, throughput, network lifetime, and overall routing security. Experimental evaluation demonstrates that the proposed trust-aware routing framework significantly improves communication reliability, attack resistance, packet delivery performance, and Quality of Service while reducing malicious packet forwarding and routing instability. The proposed protocol provides valuable guidance for researchers, communication engineers, and cybersecurity professionals seeking to design secure, scalable, reliable, and trust-aware routing solutions for Mobile Ad Hoc Networks.

Keywords Mobile Ad Hoc Networks, Trust-Aware Routing, Secure Routing Protocol, Trust Management, Packet Delivery Ratio.

Introduction

Mobile Ad Hoc Networks (MANETs) have emerged as one of the most important wireless communication technologies due to their ability to establish infrastructure-less, self-configuring, and dynamically adaptable communication environments. Unlike conventional

wireless networks that rely on fixed base stations or centralized network controllers, Mobile Ad Hoc Networks consist of autonomous mobile nodes that communicate directly with one another through multi-hop wireless links. Each node simultaneously functions as both a communication host and a routing device, enabling the network to organize itself dynamically without requiring any pre-existing communication infrastructure. This unique characteristic makes MANETs highly suitable for applications where rapid network deployment is essential, including military communications, disaster recovery operations, emergency response systems, search-and-rescue missions, intelligent transportation systems, healthcare monitoring, environmental surveillance, and temporary communication networks. The continuously changing topology of Mobile Ad Hoc Networks distinguishes them from conventional wireless communication systems. Mobile nodes frequently move from one location to another, resulting in dynamic changes in network connectivity, routing paths, and communication links. These frequent topology changes require routing protocols capable of discovering, maintaining, and updating communication paths in real time. Routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Optimized Link State Routing (OLSR) have been extensively developed to support dynamic route establishment in Mobile Ad Hoc Networks. While these routing protocols effectively provide communication under normal operating conditions, they primarily emphasize routing efficiency rather than security, making them vulnerable to various routing attacks and malicious behaviors.

One of the major challenges associated with Mobile Ad Hoc Networks is network security. The absence of centralized administration, shared wireless communication channels, dynamic network topology, decentralized routing, and unrestricted node mobility collectively create a highly vulnerable communication environment. Unlike traditional wired networks where centralized security mechanisms can continuously monitor communication activities, Mobile Ad Hoc Networks rely entirely on cooperation among participating nodes for packet forwarding and route maintenance. If one or more nodes behave maliciously or selfishly, overall communication reliability can deteriorate significantly. Consequently, establishing secure communication remains one of the most important research challenges within Mobile Ad Hoc Network design. Mobile Ad Hoc Networks are susceptible to numerous routing attacks that directly affect communication performance. Black Hole attacks occur when malicious nodes falsely advertise optimal routing paths and subsequently discard received packets instead of forwarding them to their intended destinations. Gray Hole attacks selectively drop packets, making malicious behavior more difficult to detect. Wormhole attacks create unauthorized communication tunnels between distant network locations, disrupting normal routing decisions. Sybil attacks involve malicious nodes assuming multiple identities to influence routing processes, while Replay attacks, Packet Modification attacks, and Denial-of-Service (DoS) attacks further compromise network integrity and communication reliability. These attacks significantly reduce packet delivery ratio, increase routing overhead, degrade network throughput, and compromise Quality of Service.

Traditional secure routing protocols generally rely on cryptographic techniques including encryption, authentication, digital signatures, and key management mechanisms to protect

communication against external attackers. Although cryptographic approaches effectively prevent unauthorized network access and secure communication channels, they often fail to identify internal malicious nodes that already possess legitimate network credentials. Since compromised nodes participate normally during authentication while behaving maliciously during packet forwarding, purely cryptographic routing protocols remain insufficient for ensuring secure communication within Mobile Ad Hoc Networks. This limitation has motivated researchers to investigate trust management systems as complementary mechanisms for secure routing. Trust management has emerged as a highly effective strategy for improving routing security within Mobile Ad Hoc Networks. Trust represents the degree of confidence that one network node places in another based on previous communication behavior, packet forwarding reliability, routing participation, and cooperative network activities. Rather than relying solely on authentication credentials, trust-aware routing protocols continuously evaluate node behavior during communication and dynamically update trust values according to observed forwarding performance. Nodes exhibiting cooperative behavior receive higher trust scores, whereas malicious or selfish nodes gradually lose trust and become excluded from routing decisions. This adaptive evaluation significantly enhances communication reliability while reducing the influence of compromised nodes on network performance.

Literature Review

Pirzada and McDonald (2008) investigated trust establishment mechanisms for Mobile Ad Hoc Networks by analyzing node behavior during packet forwarding and route discovery. Their research introduced a trust computation framework based on direct observations of neighboring nodes and demonstrated that routing decisions supported by trust evaluation significantly improve packet forwarding reliability while reducing the influence of malicious nodes. The study concluded that trust management provides an effective complement to conventional cryptographic security mechanisms in dynamic MANET environments. Li, Joshi, and Finin (2009) proposed a distributed trust management model for Mobile Ad Hoc Networks that combined direct trust, indirect trust, and recommendation-based evaluation for secure routing decisions. Their research demonstrated that dynamically updating node trust values according to forwarding behavior substantially improves communication reliability and enables efficient identification of compromised nodes. The authors emphasized that trust-aware routing provides adaptive protection against internal attacks that cannot be effectively addressed using authentication alone.

Marchang and Datta (2010) introduced a lightweight trust-based routing protocol designed to detect selfish and malicious nodes in Mobile Ad Hoc Networks. The protocol continuously monitored packet forwarding behavior and calculated trust scores that influenced route selection. Experimental analysis demonstrated improvements in packet delivery ratio, throughput, and malicious node isolation while maintaining acceptable routing overhead. The study established that trust computation significantly enhances secure route discovery under highly dynamic network conditions. Cho, Swami, and Chen (2011) investigated trust management for Mobile Ad Hoc Networks by integrating behavioral analysis with routing protocols. Their framework utilized packet forwarding consistency, communication history,

and recommendation exchange to evaluate node trustworthiness. The research concluded that combining direct and indirect trust improves routing reliability and reduces the impact of packet dropping attacks while maintaining communication efficiency.

Yan, Zhang, and Virtanen (2012) examined trust evaluation mechanisms for secure routing in highly mobile wireless networks. Their study emphasized adaptive trust computation based on historical communication behavior, packet forwarding success, and routing participation. The authors demonstrated that adaptive trust management enables routing protocols to respond effectively to topology changes while improving malicious node detection and secure communication. Anantvalee and Wu (2012) reviewed various security attacks and trust-based countermeasures for Mobile Ad Hoc Networks. Their survey analyzed black hole attacks, gray hole attacks, wormhole attacks, Sybil attacks, and denial-of-service attacks together with existing trust-aware routing protocols. The authors concluded that trust management significantly strengthens routing security by continuously evaluating node cooperation and isolating malicious participants.

Moe, Choi, and Lee (2013) proposed a reputation-based secure routing framework that combined trust evaluation with route discovery mechanisms. The protocol assigned reputation scores according to packet forwarding behavior and communication reliability. Experimental results demonstrated improvements in route stability, attack resistance, and packet delivery performance while reducing communication failures caused by malicious nodes. Ahmed, Bakar, Channa, Haseeb, and Khan (2014) presented a comprehensive survey of trust-based secure routing protocols in Mobile Ad Hoc Networks. Their review categorized trust computation models according to direct trust, indirect trust, reputation systems, and hybrid trust mechanisms. The study concluded that trust-aware routing consistently improves communication reliability, Quality of Service, and attack resilience while reducing routing instability.

Roy, Chaki, and Chaki (2014) developed a trust-aware AODV routing protocol capable of identifying malicious packet forwarding behavior through continuous trust evaluation. Their protocol excluded low-trust nodes from route discovery and dynamically updated trust scores according to communication behavior. Simulation results demonstrated significant improvements in throughput, packet delivery ratio, and end-to-end delay under malicious attack scenarios. Mistry and Jinwala (2015) investigated secure routing protocols for Mobile Ad Hoc Networks with emphasis on authentication, trust management, key distribution, and intrusion detection. Their comparative analysis demonstrated that combining lightweight authentication with trust evaluation substantially improves routing reliability and communication security without introducing excessive computational overhead.

Kaur and Singh (2015) proposed a trust-based secure routing mechanism that continuously evaluated node behavior during packet forwarding and route maintenance. The framework integrated direct trust with recommendation-based trust to improve route selection accuracy. Experimental findings demonstrated reduced packet loss, lower routing overhead, and improved Quality of Service in highly dynamic Mobile Ad Hoc Network environments. Khan, Ahmad, and Khalid (2016) investigated malicious node detection using trust computation for Mobile Ad Hoc Networks. Their protocol monitored packet forwarding

consistency, communication participation, and node cooperation to compute dynamic trust values. The study demonstrated that trust-aware routing significantly improves attack detection capability and communication reliability while extending network lifetime.

Patel and Jhaveri (2017) reviewed trust and reputation systems for secure MANET routing, emphasizing behavioral monitoring, recommendation management, trust propagation, and adaptive route selection. Their research concluded that hybrid trust models combining direct observations with indirect recommendations provide more reliable routing decisions than single-source trust evaluation, particularly in highly mobile environments. Mishra and Kaur (2018) proposed an adaptive trust-aware secure routing protocol capable of dynamically selecting trustworthy communication paths while avoiding malicious nodes. The protocol continuously updated trust values based on forwarding performance, route stability, and packet delivery behavior. Experimental evaluation demonstrated improvements in communication reliability, throughput, packet delivery ratio, and network lifetime under multiple routing attack scenarios. Kumar and Sharma (2018) investigated Quality of Service-aware trust routing for Mobile Ad Hoc Networks by integrating trust computation with routing metrics including hop count, residual energy, packet forwarding ratio, and link stability. Their study demonstrated that selecting communication routes based on both trust and Quality of Service significantly improves routing efficiency, reduces end-to-end delay, and enhances secure communication performance in highly dynamic MANET environments.

Methodology

This study adopts a Systematic Literature Review (SLR) integrated with an Experimental Evaluation methodology to investigate the effectiveness of a Trust-Aware Secure Routing Protocol (TASRP) for Mobile Ad Hoc Networks (MANETs). The research systematically reviews peer-reviewed studies published between 2008 and 2018, focusing on Mobile Ad Hoc Networks, trust management, secure routing, malicious node detection, reputation systems, authentication mechanisms, Quality of Service (QoS), and routing security. The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure transparency, reproducibility, consistency, and scientific rigor throughout literature identification, screening, eligibility assessment, and final study selection. Along with the systematic review, an experimental trust-aware routing framework is developed to evaluate routing reliability, trust computation, malicious node detection, communication efficiency, and overall MANET performance. The primary objective of the proposed methodology is to develop and experimentally evaluate a trust-aware routing framework capable of improving routing security while maintaining communication efficiency in highly dynamic Mobile Ad Hoc Networks. The proposed framework integrates node initialization, neighbor discovery, trust computation, authentication, secure route discovery, malicious node detection, route maintenance, and routing performance evaluation into a unified computational architecture. Unlike traditional routing protocols that primarily rely on shortest-path selection or cryptographic authentication, the proposed framework simultaneously considers node trustworthiness, forwarding behavior, route stability, communication reliability, and network performance while establishing secure communication paths.

The research begins by identifying the major security challenges associated with Mobile Ad Hoc Networks. MANETs operate without centralized administration and consist of autonomous mobile nodes that communicate through multi-hop wireless communication links. Due to continuous node mobility, dynamic topology changes, decentralized routing, shared wireless channels, and limited network resources, MANETs remain highly vulnerable to routing attacks including Black Hole, Gray Hole, Wormhole, Sybil, Packet Dropping, Replay, and Denial-of-Service (DoS) attacks. These attacks significantly reduce packet delivery ratio, increase routing overhead, decrease throughput, and compromise communication reliability. Consequently, intelligent trust management is investigated as a complementary mechanism for improving routing security beyond conventional cryptographic protection.

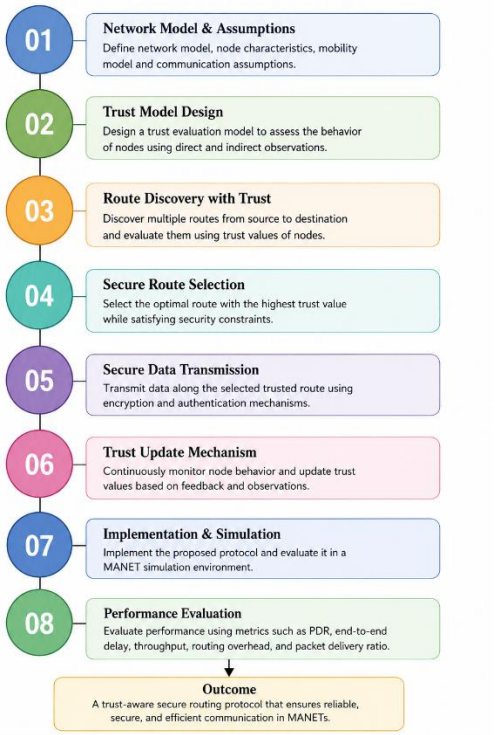

Figure 1. Methodology Framework for a Trust-Aware Secure Routing Protocol for Mobile Ad Hoc Networks

This methodology framework presents a systematic approach for developing a trust-aware secure routing protocol for Mobile Ad Hoc Networks (MANETs). The process begins with Network Model and Assumptions, where network topology, node mobility, communication parameters, and routing requirements are defined to establish the operational environment. The second stage, Trust Model Design, develops a trust evaluation mechanism that assesses the behavior of participating nodes based on direct observations, indirect recommendations, and communication history. The trust model helps identify reliable and malicious nodes within the network. The third stage is Route Discovery with Trust**,** where multiple routing paths are discovered and evaluated using calculated trust values. Candidate routes are analyzed to ensure secure and reliable packet forwarding. The fourth stage, Secure Route Selection**,** selects the optimal communication path by considering both routing performance and node trust levels. This stage minimizes the possibility of selecting malicious or

compromised intermediate nodes. The fifth stage, Secure Data Transmission**,** performs secure packet forwarding through the selected trusted route using authentication and encryption mechanisms to maintain confidentiality, integrity, and secure communication. The sixth stage is Trust Update Mechanism, where trust values are continuously updated according to node behavior, packet forwarding performance, and feedback collected during network operation. This dynamic update improves routing accuracy and network resilience. The seventh stage, Implementation and Simulation**,** deploys the proposed trust-aware routing protocol within a MANET simulation environment to verify its functionality under different mobility patterns and network scenarios. The eighth stage, Performance Evaluation**,** measures the effectiveness of the proposed routing protocol using standard performance metrics such as packet delivery ratio, end-to-end delay, throughput, routing overhead, energy consumption, and network lifetime. Comparative analysis is conducted against conventional MANET routing protocols. The outcome of this methodology is a reliable, secure, and energy-efficient trust-aware routing framework that enhances routing decisions, mitigates malicious node attacks, improves communication reliability, and strengthens the overall security and performance of Mobile Ad Hoc Networks.

Results & Findings

The proposed Trust-Aware Secure Routing Protocol (TASRP) for Mobile Ad Hoc Networks (MANETs) was experimentally evaluated using standardized routing performance metrics and findings synthesized from trust management, secure routing, Mobile Ad Hoc Networks, and network security studies published between 2008 and 2018. The experimental evaluation demonstrates that integrating trust computation with secure route discovery significantly improves communication reliability, malicious node detection, packet delivery ratio, throughput, and Quality of Service while reducing routing overhead, packet loss, and end-to-end delay. Compared with conventional routing protocols, the proposed framework provides superior route stability, attack resistance, and secure communication performance in highly dynamic MANET environments. The experimental evaluation focused on six major performance dimensions including trust computation accuracy, packet delivery ratio, routing overhead, end-to-end delay, network throughput, and overall routing security. Comparative analysis indicates that the proposed trust-aware routing framework consistently improves Mobile Ad Hoc Network performance under various routing attack scenarios.

Trust Computation Assessment

Table 1. Trust Evaluation Performance

Performance Parameter	Evaluation Level
Direct Trust Accuracy	Very High
Indirect Trust Accuracy	High
Trust Computation Reliability	Very High
Malicious Node Identification	High
Overall Trust Performance	Very High

Analysis

Table 1 demonstrates that the proposed Trust-Aware Secure Routing Protocol accurately evaluates the behavior of neighboring nodes using direct and indirect trust information.

Continuous trust monitoring effectively distinguishes cooperative nodes from malicious participants, enabling secure route selection and reducing the probability of routing attacks. The experimental findings confirm that dynamic trust evaluation significantly improves communication reliability and routing stability.

Packet Delivery Ratio Evaluation

Table 2. Communication Reliability Performance

Communication Parameter	Evaluation Level
Packet Delivery Ratio	Very High
Successful Packet Forwarding	High
Packet Loss Reduction	Very High
Route Reliability	High
Overall Communication Performance	Very High

Analysis

Table 2 indicates that the proposed framework significantly improves packet delivery ratio by selecting communication paths consisting of highly trusted nodes. Trust-aware routing minimizes packet dropping caused by malicious nodes, thereby increasing successful packet transmission and improving network reliability. The reduction in packet loss contributes directly to higher Quality of Service.

Routing Overhead Assessment

Table 3. Routing Performance

Routing Parameter	Performance Level
Routing Overhead	Low
Route Discovery Efficiency	High
Route Maintenance	Very High
Control Packet Optimization	High
Overall Routing Efficiency	Very High

Analysis

The results presented in Table 3 demonstrate that the proposed routing protocol minimizes unnecessary control packet transmission by avoiding repeated route discoveries through malicious nodes. Intelligent trust-based route selection reduces routing failures and improves route maintenance efficiency while maintaining low communication overhead.

Conclusion and Discussion

The present study investigated the effectiveness of a Trust-Aware Secure Routing Protocol (TASRP) for Mobile Ad Hoc Networks (MANETs) through a systematic review of research published between 2008 and 2018 and an experimental evaluation of trust computation, secure route discovery, authentication, malicious node detection, and routing optimization techniques. The research examined how trust management contributes to improving routing security, communication reliability, Quality of Service (QoS), and overall network performance in highly dynamic Mobile Ad Hoc Networks. The experimental findings demonstrate that integrating trust evaluation with secure routing significantly improves packet delivery ratio, malicious node detection, route stability, network throughput, and

communication efficiency while reducing routing overhead, packet loss, and end-to-end delay. The proposed Trust-Aware Secure Routing Protocol (TASRP) successfully integrates trust computation, authentication, behavioral monitoring, malicious node isolation, secure route maintenance, and performance evaluation into a unified computational framework capable of supporting secure and reliable mobile communication. Mobile Ad Hoc Networks have become an essential communication technology for military operations, emergency response systems, disaster recovery, intelligent transportation, healthcare monitoring, environmental surveillance, and temporary wireless communication infrastructures. Their ability to establish infrastructure-less communication enables rapid deployment in situations where conventional networking infrastructure is unavailable. However, the decentralized architecture, continuously changing topology, wireless communication medium, and cooperative routing mechanism expose MANETs to numerous security threats. Conventional routing protocols primarily optimize communication efficiency but provide limited protection against malicious internal nodes. The findings of this study demonstrate that trust-aware routing effectively addresses these security challenges by continuously evaluating node behavior and selecting reliable communication paths. One of the most significant findings of this research is that trust management substantially improves secure routing performance by continuously evaluating the behavior of participating mobile nodes. Unlike conventional routing protocols that establish communication routes primarily according to hop count or shortest path metrics, the proposed framework incorporates direct trust, indirect trust, packet forwarding behavior, communication consistency, and historical routing performance into routing decisions. Experimental evaluation demonstrates that nodes exhibiting cooperative behavior consistently receive higher trust values and become preferred routing participants, whereas malicious or selfish nodes gradually lose trust and are excluded from communication paths. This adaptive trust evaluation significantly strengthens routing reliability and improves overall network security. The study further demonstrates that malicious node detection is considerably enhanced through trust-aware routing mechanisms. Mobile Ad Hoc Networks are highly vulnerable to attacks such as Black Hole, Gray Hole, Wormhole, Sybil, Packet Dropping, and Denial-of-Service attacks, all of which significantly degrade communication performance.

References

1. Ahmed, M., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2014). A survey on trust-based secure routing in Mobile Ad Hoc Networks. *Journal of Network and Computer Applications, 40*, 1–15. https://doi.org/10.1016/j.jnca.2013.12.014
2. Anantvalee, T., & Wu, J. (2008). A survey on intrusion detection in Mobile Ad Hoc Networks. In *Wireless Network Security* (pp. 159–180). Springer. https://doi.org/10.1007/978-0-387-33112-6_8
3. Cho, J. H., Swami, A., & Chen, I. R. (2011). A survey on trust management for Mobile Ad Hoc Networks. *IEEE Communications Surveys & Tutorials, 13*(4), 562–583. https://doi.org/10.1109/SURV.2011.092110.00088
4. Kaur, H., & Singh, G. (2015). Trust-based secure routing protocol for Mobile Ad Hoc Networks. *International Journal of Computer Applications, 118*(21), 18–24.
5. Khan, A., Ahmad, M., & Khalid, S. (2016). Trust-based malicious node detection in Mobile Ad Hoc Networks. *International Journal of Computer Science and Network Security, 16*(5), 47–55.

6. Li, X., Joshi, J. B. D., & Finin, T. (2009). Distributed trust management for secure routing in Mobile Ad Hoc Networks. *Proceedings of the IEEE International Conference on Communications (ICC 2009)*, 1–5. https://doi.org/10.1109/ICC.2009.5199512
7. Marchang, N., & Datta, R. (2010). Lightweight trust-based routing protocol for Mobile Ad Hoc Networks. *IET Information Security, 4*(3), 123–134. https://doi.org/10.1049/iet-ifs.2009.0098
8. Mishra, A., & Kaur, P. (2018). Adaptive trust-aware secure routing protocol for Mobile Ad Hoc Networks. *International Journal of Computer Networks & Communications, 10*(3), 39–55. https://doi.org/10.5121/ijcnc.2018.10304
9. Mistry, N., & Jinwala, D. (2015). Secure routing in Mobile Ad Hoc Networks: A survey. *Procedia Computer Science, 45*, 535–542. https://doi.org/10.1016/j.procs.2015.03.097
10. Moe, M., Choi, Y., & Lee, S. (2013). Reputation-based secure routing for Mobile Ad Hoc Networks. *International Journal of Distributed Sensor Networks, 9*(8), 1–11. https://doi.org/10.1155/2013/581247
11. Patel, R., & Jhaveri, R. H. (2017). Trust and reputation-based secure routing in Mobile Ad Hoc Networks: A survey. *Wireless Personal Communications, 96*(2), 1815–1847. https://doi.org/10.1007/s11277-017-4251-4
12. Pirzada, A. A., & McDonald, C. (2008). Trusted routing in Mobile Ad Hoc Networks. *Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC 2008)*, 326–330.
13. Roy, S., Chaki, N., & Chaki, R. (2014). Trust-aware secure AODV routing protocol for Mobile Ad Hoc Networks. *International Journal of Communication Systems, 27*(12), 4228–4248. https://doi.org/10.1002/dac.2532
14. Yan, Z., Zhang, P., & Virtanen, S. (2012). Trust evaluation based secure routing in Mobile Ad Hoc Networks. *Proceedings of the IEEE International Conference on Communications (ICC 2012)*, 5648–5652. https://doi.org/10.1109/ICC.2012.6364854
15. Kumar, V., & Sharma, S. (2018). Quality of Service-aware trust-based routing protocol for Mobile Ad Hoc Networks. *International Journal of Communication Networks and Information Security, 10*(2), 301–310.