JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Intelligent and Secure Routing Protocols for Resilient Mobile Ad Hoc Networks

Dr. Mayank Kumar

Assistant Professor, Department of Computer Science, Arunachal University of Studies, Namsai, Arunachal Pradesh

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are inherently vulnerable to a variety of security threats due to their decentralized and dynamic nature. Among these, Byzantine attacks are particularly disruptive, where malicious nodes-either individually or in groups-compromise the routing path between the source and destination, leading to significant performance degradation. To address this issue, this paper introduces a novel mitigation strategy based on the Cohen Kappa Reliability Coefficient (CKRCM). The approach involves continuous monitoring of intermediate nodes by their neighboring nodes using timestamp-based observations. If an acknowledgment is not received within a specified timeframe, the corresponding node is flagged as potentially compromised. The method further assesses node trustworthiness by calculating individual trust and reliability metrics. Experimental results demonstrate that the proposed CKRCM mechanism achieves superior performance compared to existing solutions, particularly in terms of throughput, packet delivery ratio (PDR), and packet loss ratio (PLR).

Keywords : MANET, Byzantine Attack, Cohen Kappa Reliability Coefficient, Trust Factor, Reliability

1.INTRODUCTION

Recent advancements in wireless communication have significantly contributed to the rapid expansion of mobile communication technologies. The widespread adoption of cost-effective devices such as laptops, wireless modems, and high-speed wireless Local Area Networks (LANs) has played a crucial role in this evolution. Due to their lightweight and portable nature, these devices offer enhanced mobility and convenience to users. Consequently, mobile users increasingly favor wireless networks over traditional wired systems, as they provide seamless and uninterrupted connectivity.

1.1 Adhoc Networks

Unlike traditional infrastructure-based networks, ad hoc networks operate without the need for Base Stations (BSs). They enable flexible, on-the-go computing by facilitating wireless communication among devices equipped with networking capabilities. Functioning as a type of Local Area Network (LAN), ad hoc networks are self-configurable and do not rely on any fixed infrastructure, allowing them to be established and maintained dynamically. In these networks, data transmission is managed collaboratively by the nodes themselves, as each node is responsible for forwarding packets to other nodes without depending on centralized control.

1.2 Mobile Ad Hoc Network

The various sectors in the field of wireless communication include cellular telephony, satellite- based communication and Wireless Local Area Networks (WLANs).There are two different categories that are described by the IEEE 802.11 standard of wireless networks for WLANs built on the structure namely, infrastructure-based and infrastructure-less (ad hoc) networks. APs establish communication between the mobile nodes and wired networks [1].

2.TOPOLOGY

The topology changes are frequent and unpredictable due to the dynamic nature of the nodes, thus leading to an increase in the routing overhead. Routing is an uphill task as finding an efficient path to the destination depends on various factors like Residual Energy (RE), Received Signal Strength (RSS) of the next hop node, topology, location of the request initiator and so on. Routing is an important area that demands much attention. There are a number of routing protocols available in the literature. They are broadly classified into the following.

✓Topology based approach
✓Location based approach
✓Power/energy aware approach

2.1 Reactive Routing Protocols

Reactive routing protocols, often referred to as "on-demand routing" protocols, establish routes only when required, as they do not maintain continuous routing information for all nodes in the network. A communication path is discovered only when a node initiates data transmission to another node.

In contrast to proactive routing protocols-which generate significant control overhead due to the constant exchange of routing information to cope with dynamic link changes-reactive protocols minimize overhead by initiating route discovery only when necessary. When a node intends to send data, it first checks its routing table for an existing path. If no route is found, a route discovery process is triggered.

During this discovery phase, the source node broadcasts a Route Request (RREQ) packet to its neighboring nodes. This packet continues to propagate through the network until it reaches the destination node. Upon receiving the RREQ, the destination node replies with a unicast Route Reply (RREP) packet, which is sent back to the source. Once the route is established, the protocol enters the route maintenance phase to ensure the path remains valid during communication.

2.2 Power or Energy-Aware Approach

COMmonPOWer (COMPOW) is an energy-efficient routing protocol designed to optimize power consumption in wireless networks. In this protocol, the wireless interface maintains a separate routing table for each transmission power level. To build these tables, nodes periodically exchange Hello messages at various power levels. The size of each routing table is determined by the number of neighboring nodes that are reachable at that specific power level.

The final entry in each routing table reflects the total number of nodes accessible when the node transmits at maximum power. After evaluating all power levels, the protocol determines the optimal transmission power that ensures network connectivity with minimal energy usage. This optimal level is then used to generate a master routing table that guides communication within the network.

3.RELATED WORK

Several researchers have contributed to the development of techniques for mitigating Byzantine attacks in network environments, particularly in Mobile Ad Hoc Networks (MANETs).

Perlman (1988) conducted foundational work on Byzantine failures within the network layer, highlighting the challenges they pose in terms of increased communication costs and computational overhead. The study introduced two methods to address these issues: one employing a flooding-based path discovery mechanism, and the other utilizing a link-state approach to manage routing information.

Awerbuch et al. (2003) proposed a novel secure routing method leveraging the Swarm Intelligence paradigm and Distributed Reinforcement Learning. Their model uses reverse-ordered Hash Message Authentication Codes (HMACs) to ensure packet authenticity and integrity. In this approach, the source node maintains a dynamic probability graph to track the likelihood of successful data delivery to the destination. Intermediate nodes are assigned the task of forwarding packets and returning acknowledgments, but are restricted from making independent hop-by-hop routing decisions, thereby minimizing the risk of route tampering.

Further research by Awerbuch et al. (2005) focused on the On-Demand Secure Byzantine Resilient Routing (ODSBR) protocol. Their work involved analyzing the protocol’s steady-state performance under various Byzantine attack models, providing deeper insights into its robustness and adaptability in adversarial scenarios.

3.1 Secured Routing Protocol for Byzantine Attacks

Castro et al. (2002) proposed a solution to combat Byzantine attacks by employing routing along multiple paths. While this redundant routing strategy increases resilience, it also incurs higher costs. Additionally, iterative routing methods introduce challenges in verifying the correctness of each routing step. To address these issues, Castro et al. incorporate cryptographic techniques for verification, ensuring the integrity of the routing process. However, the protocol does not account for bogus requests that unnecessarily consume network resources.

In another significant contribution, Awerbuch et al. (2002) introduced the On-Demand Secure Byzantine

Resilient (ODSBR) routing protocol for MANETs. This protocol is designed to be robust against both outsider and Byzantine attacks. The source node in this framework is equipped with comprehensive knowledge of the network's nodes and has the ability to effectively monitor their behavior. The protocol establishes strict bounds on the potential damage a Byzantine node can inflict on the network, providing a safeguard against malicious actions regardless of the attacker's behavior.

CONCLUSION

In conclusion, various strategies have been proposed to mitigate Byzantine attacks in network routing. Techniques such as multi-path routing, cryptographic verification and behavior monitoring are crucial in enhancing the security and reliability of networks, particularly in mobile ad hoc environments. While solutions like Castro et al.'s redundant routing and Awerbuch et al.'s ODSBR protocol provide significant improvements, challenges remain in minimizing overhead and preventing resource wastage. Ongoing research continues to refine these protocols, aiming for more efficient and resilient routing mechanisms in the face of adversarial attacks.

REFERENCES

1.Perlman, R., "Interconnections: Bridges, Routers, Switches, and Internetworking," 2nd ed., Addison-Wesley, 1988.

2.Awerbuch, B., Cidon, I., & Kolb, E., "Swarm Intelligence and Distributed Reinforcement Learning for Secure Routing in Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 278-290, Oct-Dec 2003.

3.Awerbuch, B., Cidon, I., & Kolb, E., "Evaluation of On-Demand Secure Byzantine Resilient Routing in Ad Hoc Networks," *Proceedings of the International Conference on Networking*, 2005, pp. 118-132.

4.Castro, M., et al., "Securing Routing Protocols for Ad Hoc Networks Against Byzantine Attacks," *Proceedings of the International Conference on Mobile Computing and Networking*, 2002, pp. 107-118.

5.Awerbuch, B., Cidon, I., & Kolb, E., "On-Demand Secure Byzantine Resilient Routing for Mobile Ad Hoc Networks," *Proceedings of the International Conference on Distributed Computing Systems*, 2002, pp. 210-220.