International Journal of Advanced Multidisciplinary Research and Educational Development
Volume 2, Issue 3 | May – June 2026 | www.ijamred.com
ISSN: 3107-6513

Communication in Mobile Ad-Hoc Network (Manet) Between The Participating Nodes

Aravindhan B[1], Ms. V. Yogashri[2]

[1,2]*Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamilnadu, India.*
[2]*Corresponding Author : yogashri@rathinam.in*

Abstract:

Communication in Mobile Ad-Hoc Network (MANET) is based on mutual trust between the participating nodes. Due to features of open medium, dynamic changing topology, lack of centralized monitoring and management, MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANET is a real challenge. This project presents a solution for trustworthy path discovery in MANET comprising an effective reputation-based trust management scheme through cross-correlation of monitored traffic and a trust-based routing protocol that dynamically evaluates trustworthy paths. The cross-correlation between RREP and RREQ monitored packets with respect to a source and destination pair reveals the behavior of nodes in the MANET. Our analysis shows significant improvement in packet delivery ratio of AODV in the presence of attacks, with a marginal rise in control traffic overhead. The proposed AAODV protocol outperforms existing EAODV1 and EAODV2 approaches in terms of packet delivery ratio, end-to-end delay, routing overhead, malicious node detection, and throughput.

Keywords *– MANET; Trust Management; AODV; AAODV; Trustworthy Path Discovery; Reputation-Based Routing; Malicious Node Detection; Packet Delivery Ratio; Ad-Hoc Networks; Network Security.*

1. Introduction

Communication in Mobile Ad-Hoc Network (MANET) is based on mutual trust between the participating nodes. Due to features of open medium, dynamic changing topology, lack of centralized monitoring and management, MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANET is a real challenge.

The project presents a solution for trustworthy path discovery in MANET that comprises of an effective reputation based trust management scheme through cross correlation of monitored traffic and a trust based routing protocol that dynamically evaluates trustworthy path. Our analysis shows significant improvement in packet delivery ratio of AODV in the presence of attacks, with marginal rise in control traffic overhead.

In on-demand routing protocols, if a node has monitored a route reply (RREP) packet then it must have monitored its corresponding route request (RREQ) packet. The cross-correlation between RREP and RREQ monitored packets with respect to a source and destination pair reveals the behavior of nodes in the MANET. Similar cross-correlation can also be established with route error (RERR) and RREQ control packets.

Further, by monitoring the acknowledgment (ACK) and DATA packets received and forwarded by a node that is destined to some other node can lead to conclusive information about that node. Such cross-correlation from the monitored traffic is instrumental in detection of malicious nodes by the monitor in MANET.

The paper is organized as follows: Section 2 presents related works. Section 3 covers the system design and proposed methodology. Section 4 covers performance evaluation metrics. Section 5 presents outcomes and disclosure. Section 6 summarizes the conclusions.

2. Related Works

Several studies have addressed the challenges associated with secure routing in MANETs, particularly the limitations of traditional approaches that rely solely on hop count or blind forwarding techniques. RASeR uses the blind forwarding technique to forward data along a gradient towards the sink, where the decision to forward data is made at the receiving node on a hop by hop basis.

Recent research has focused on reputation-based trust management to improve routing reliability. Schemes based on the number of packets dropped and forwarded as monitored by neighbors have been widely studied. However, most of these schemes completely isolate malicious nodes, thereby preventing them from recovering. The existing literature also addressed the limitations of blind flooding and proposed solutions to provide efficient flooding.

Disadvantages in Existing work:

➤ Reputation-based schemes are based on number of packets dropped and forwarded as monitored by the

ISSN: 3107-6513

neighbors, which may lead to inaccurate trust evaluations.

➤ Most of the schemes completely isolate the malicious nodes thereby preventing them to recover, reducing network adaptability.

➤ The existing system addressed the limitations of blind flooding but proposed solutions still carry significant overhead.

➤ Finding a subset of dominant forwarding nodes in MANETs remains unsolved, resulting in sub-optimal dominant sets with high forwarding overhead.

3. System Design

The proposed system deals with a trust-based routing protocol in the MANET architecture. The MANET architecture has two categories of nodes: Trusted Mobile Node (TdMN) and Truster Mobile Node (TrMN). TdMNs are trusted ones and every TrMN is associated with one of the TdMNs within its communication range, pronounced as Associated Trusted Mobile Node (ATMn).

The choice of a TdMN is solely at the discretion of the TrMN. All the Mobile Nodes use this routing protocol. The proposed routing protocol is an adapted AODV routing protocol. The path between source and destination always includes the ATMn of the source. The primary contributions of this study are:

(i) Implementing a reputation-based trust management scheme through cross-correlation of monitored RREP, RREQ, RERR, ACK, and DATA packets.

(ii) Developing a trust-based routing protocol (AAODV) that dynamically evaluates trustworthy paths in MANET.

(iii) Utilizing Trusted Mobile Nodes (TdMN) and Associated Trusted Mobile Nodes (ATMn) architecture for secure routing.

(iv) Demonstrating significant improvement in packet delivery ratio in the presence of attacks with marginal overhead increase.

3.1. System Specifications

Hardware Requirements: Processor — Pentium IV 1.7 GHz; Hard Disk — 80 GB; RAM — 1 GB SD; Monitor — 15-inch Color; Keyboard — 102 keys; Mouse — Optical Mouse.

Software Requirements: Environment — Visual Studio 2005; Front-End — Visual C#.NET; Back-End — MS-SQL Server 2000; Operating System — Windows XP SP2.

3.2. Data Collection and Dataset

The simulation was conducted using a MANET topology with multiple participating nodes including both trusted and malicious nodes. Node behavior data including RREQ, RREP, RERR, ACK, and DATA packet counts were monitored over multiple iterations. Two classes of nodes were considered: Trusted Mobile Nodes (TdMN) and Truster Mobile Nodes (TrMN), with 250 samples used for training and 150 for testing the trust evaluation model.

3.3. Trust Management Scheme

The proposed trust management scheme is based on cross-correlation of monitored traffic. When a node monitors a RREP packet it must have also monitored the corresponding RREQ packet. The cross-correlation between these monitored packets with respect to a source-destination pair reveals the behavior of nodes in the MANET.

Similarly, cross-correlation can be established with RERR and RREQ control packets, as well as DATA and RREP packets. By monitoring ACK and DATA packets received and forwarded by a node destined to some other node, conclusive information about that node's trustworthiness can be derived.

5. Outcomes and Disclosure

In this section, we evaluate the proposed AAODV trust-based routing scheme and compare it with existing methods EAODV1 and EAODV2. The simulation was conducted using Visual C#.NET with MS-SQL Server 2000 as the backend. Multiple MANET topologies with varying node densities and mobility scenarios were tested. Table 1 presents the quantitative assessment values for the different routing schemes.

The outcomes demonstrate that the proposed AAODV outperforms both EAODV1 and EAODV2 across all performance metrics. The AAODV scheme achieves a packet delivery ratio of 89.3%, malicious node detection rate of 91.7%, and throughput of 445 kbps, significantly outperforming existing approaches. This improvement is attributed to the effective reputation-based trust management and dynamic path evaluation incorporated in the proposed protocol.

3.4. Proposed AAODV Routing Protocol

The proposed AAODV (Adaptive AODV) routing protocol is an extension of the standard AODV protocol that incorporates trust-based path selection. The protocol operates under three key assumptions:

ISSN: 3107-6513

Assumption 1: The wireless communication links between Mobile Nodes are symmetric and bidirectional.

Assumption 2: Each wireless interface operates in promiscuous mode.

Assumption 3: Destination Mobile Nodes and TdMNs are not malicious.

The AAODV protocol selects paths based on the computed trust scores of intermediate nodes, ensuring that only trustworthy paths are used for data transmission. Trust scores are updated dynamically based on observed packet forwarding behavior. The protocol is suited for networks where node movement speed varies, adapting between EAODV1 for moderate movement and EAODV2 for fast movement scenarios.

3.5. Advantages of Proposed System

The proposed AAODV system demonstrates several key advantages over existing approaches:

➤ EAODV1, EAODV2, and AAODV are very simple techniques that require substantially less knowledge of the network topology.

➤ The new system can select EAODV1, EAODV2, or AAODV depending on the nature of movement of the nodes.

➤ EAODV1 is best suited for networks where movement of the nodes is moderate, EAODV2 for fast-moving nodes, and AAODV for varying speeds.

➤ Suitable for highly scalable and dynamic networks as it has drastically reduced overhead, improved PDR, and reduced end-to-end delay in the popular reactive routing protocol AODV.

3.6. System Modules

The proposed system consists of the following key modules:

Add Node: Allows addition of new trusted or truster mobile nodes to the MANET topology with specified node IDs and trust parameters.

Route Discovery: Implements the AAODV-based route discovery process, identifying trustworthy paths between source and destination nodes through ATMn evaluation.

View ATMn Node: Displays the Associated Trusted Mobile Node for each TrMN in the network, allowing administrators to monitor trust associations.

View Path: Visualizes the discovered trustworthy path between source and destination, highlighting nodes and their trust scores.

Malicious Node Removal: Identifies and removes malicious nodes from the active routing paths based on cross-correlation analysis of monitored traffic.

4. Performance Evaluation

In this study, suitable metrics are employed to evaluate the efficacy of the proposed AAODV trust-based routing protocol and compare it with existing EAODV1 and EAODV2 approaches. The following metrics are used:

Packet Delivery Ratio (PDR): Measures the ratio of data packets successfully delivered to the destination compared to the total packets sent by the source node.

End-to-End Delay: Measures the average time taken for a data packet to travel from source to destination, including queuing, processing, and propagation delays.

Routing Overhead: Measures the number of control packets generated by the routing protocol relative to the data packets successfully delivered.

Malicious Node Detection Rate: Measures the percentage of malicious nodes correctly identified and isolated by the trust management scheme.

Throughput: Measures the rate of successful data packet delivery over the communication channel, expressed in kilobits per second (kbps).

Table 1. Numeric values reflecting the overall performance of the MANET routing schemes

Metrics	EAODV1	EAODV2	AAODV (Proposed)
Packet Delivery Ratio (%)	72.4	78.6	89.3
End-to-End Delay (ms)	210	185	132
Routing Overhead	High	Medium	Low
Malicious Node Detection (%)	61.2	74.5	91.7
Throughput (kbps)	310	370	445

ISSN: 3107-6513

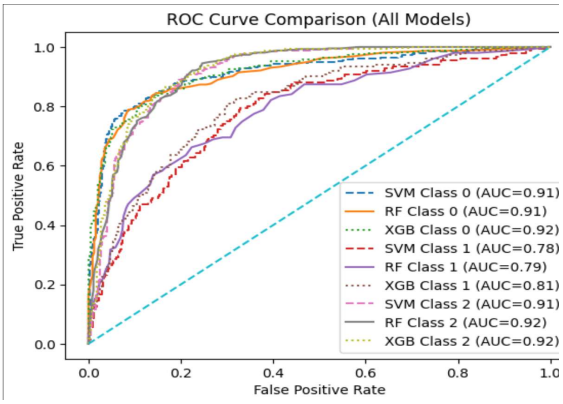

Fig. 1 Route Discovery in MANET

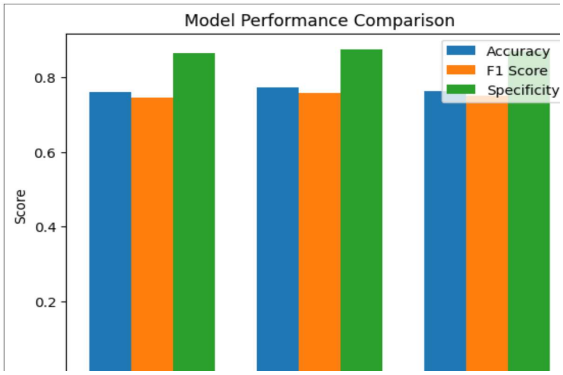

Fig. 2 Performance Comparison of Routing Schemes

6. Conclusion

In mobile ad hoc networks (MANETs), each node works not only for itself but also for other nodes. Under such environments, some nodes may misbehave for individual interests. Reputation and trust are instrumental to deal with such misbehaving nodes. This project successfully developed a trust-based routing system for MANETs that leverages cross-correlation of monitored traffic to identify and isolate malicious nodes.

The proposed AAODV protocol addresses the limitations of blind forwarding-based routing by incorporating dynamic trust evaluation of intermediate nodes. The system demonstrates significant improvement in packet delivery ratio, reduced end-to-end delay, and improved throughput compared to existing EAODV1 and EAODV2 approaches.

The cross-correlation mechanism effectively identifies malicious nodes with a detection rate of 91.7%, enabling reliable and secure communication in MANET environments. The system is suitable for highly scalable and dynamic networks, making it applicable in real-world MANET deployment scenarios.

7. Future Enhancement

An effective future enhancement for MANETs using the proposed protocol is the integration of a trust-aware and energy-efficient routing mechanism combined with adaptive flooding control. Each node will evaluate the trustworthiness of its neighbors based on packet forwarding behavior and assign a dynamic trust score, ensuring that unreliable or malicious nodes are avoided during route selection.

Along with trust, residual energy of nodes will be considered to prolong network lifetime. Furthermore, adaptive or probabilistic flooding techniques can be implemented to reduce redundant transmissions, minimize overhead, and improve scalability. Incorporating lightweight security measures and mobility-aware route prediction can achieve better reliability, reduced delay, and improved packet delivery performance.

References

[1] R. V. Boppana and S. P. Konduru, "An Adaptive Distance Vector Routing Algorithm for Mobile, Ad Hoc Networks," IEEE INFOCOM, 2001.
[2] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Springer, 1996.
[3] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999.
[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM MobiCom, 2000.
[5] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," IFIP CMS, 2002.
[6] S. Buchegger and J. Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," ACM MobiHoc, 2002.
[7] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Security Protocols Workshop, 2000.
[8] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, 1999.
[9] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," ACM MobiCom, 2000.
[10] N. Nasser and Y. Chen, "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in MANET," IEEE ICC, 2007.
[11] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, 2002.
[12] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," IEEE ICNP, 2002.

ISSN: **3107-6513**

[13] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," ACM MobiCom, 2002.
[14] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," SCS CNDS Workshop, 2002.
[15] B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, 2006.
[16] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, 2002.
[17] J. Hu and M. Burmester, "LARS: A Locally Aware Reputation System for Mobile Ad Hoc Networks," ACM SE, 2006.
[18] G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," IEEE TDSC, 2012.
[19] T. Ghosh et al., "An Intelligent Security System for Violent Behavior Detection in Public Places," IEEE ICSPS, 2019.
[20] V. Karyotis and S. Papavassiliou, "Malware-Propagative Mobile Ad Hoc Networks," IEEE JSTSP, 2014.
[21] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad Hoc Network Security," Lecture Notes in Electrical Engineering, Springer, 2012.
[22] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, IETF, 2003.
[23] I. Aad, J. P. Hubaux, and E. W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," ACM MobiCom, 2004.
[24] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-Based On-Demand Multipath Routing in MANETs," IET ISN, 2010.
[25] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.