INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

SRDAODV: A Hybrid Secure Routing Protocol for Mobile Ad-Hoc Networks

J Viji Gripsy[1,2]*, A Jayanthiladevi[3], N Mahendiran[4], A Sheela Rini[5]

1 Post- Doctoral Research Fellow, Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India
2 Associate Professor, Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, Tamilnadu, India
3 Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India
4 Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India
5 Assistant Professor, Department of Computer Science (PG), PSGR Krishnammal College for Women, Coimbatore, India

OPEN ACCESS

Received: 22-05-2023
Accepted: 16-07-2023
Published: 29-08-2023

Citation: Gripsy JV, Jayanthiladevi A, Mahendiran N, Rini AS (2023) SRDAODV: A Hybrid Secure Routing Protocol for Mobile Ad-Hoc Networks. Indian Journal of Science and Technology 16(32): 2574-2579. https://doi.org/10.17485/IJST/v16i32.1240

* **Corresponding author**.

vijigripsy@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To counteract grey hole and black hole attacks, the proposed method deploys a hybrid framework along with the Ad hoc on-demand distance vector (AODV) routing protocol. A modified protocol is called as SRD-AODV (Secure Route Discovery-Adhoc On-Demand Distance Vector). **Methods:** The proposed work establishes secure route from secure node discovery, which protects from sequential attacks. The proposed framework has three significant components Node Authentication, Secure Neighbor discovery and route establishment, and Node Isolation system. **Findings:** Performance metrics like packet delivery ratio and delay are used to assess this protocol's effectiveness. The SRD-AODV protocol contrasts with other active protocols as well as AODV. SRD-AODV has a PDR that is greater by 4.92% than EDRI-AODV and 12.23% than AODV because it excludes network attacks, has flawless routes, and prevents packets drop or connections fail. This is because SRD-AODV has more perfect routes. The proposed SRD-AODV algorithm achieves 58.5% less E2E delay than AODV and 44.5% less than EDRI-AODV. **Novelty:** This protocol uses a variety of elements and techniques to establish efficient authentication using Elliptic Curve Diffie-Hellman algorithm (ECDHA) techniques, offering both proactive and reactive solutions. Additionally, this tries to secure the data packets and routing table information. Finally, it also aims to identify and stop incursions from sequential attacks in MANET.

Keywords: MANET; AODV; Black hole attack; Grey hole attack; Denial of Service

1 Introduction

The wireless network is widely used in a variety of applications. This marvelous growth is achieved because of the MANET nature such as dynamic infrastructure, instant topology[(1)]. The network generation can be dynamic and can set up anytime and

anywhere. This tremendous degree of flexibility obviously causes a number of network security and performance problems. The procedure in MANET is threatened by a number of security flaws in diverse situations. Greyhole and blackhole attacks, which become examples of sequence number attacks, are dangerous attacks that seriously impair the network's ability to function and execute in a variety of scenarios [2]. Sequence number attacks and black hole attacks destroy certain count of data packets and discard them by deploying false route and modifying the routing information.

Black hole denial-of-service attacks include the addition of a rogue node to a network. The nearest designated destination node, this node responds to the source node's HELLO message. To keep each other informed and facilitate data flow, nodes in a packet network routinely broadcast traffic status and location updates. [3,4]. By pretending to be the destination and accepting the payload from the source node, the malicious node may try to launch a black hole attack by rerouting it. Utilizing network resources to resend the missing payload to the destination may be necessary [5,6].

Similar to black hole attacks, grey hole attacks involve a rogue node impersonating a trustworthy node and redirecting traffic. Retransmission of the lost data is requested by the network, which causes a delay and network failure. Attacks using grey holes damage and use up network resources. In contrast to black hole attacks, grey hole attacks focus on signaling data or a certain packet size [7]. Because the malicious node may only redirect a small portion of traffic or data, it might fool other network nodes into thinking it is a genuine node, making grey hole attacks challenging to detect and prevent.

Two-way handshakes are used in synchronized flooding attacks to cause denial-of-service. In a network pair, a malicious node sends the target node a number of requests, and the target node tries to answer to each one. The target's high request volume lengthens the wait and gives the impression that it is busy [8,9]. This can impede the target from properly responding to legitimate requests or processing them.

To encrypt communications over wide networks, [10] proposed utilizing a virtual private network (VPN). Numerous machine learning techniques, such as Random Forests and Nave Bays, may be used to both identify and stop malicious assaults. The limitation of this approach is required to evaluate these tactics in practical settings and identify the most effective algorithms for various networks and data.

Many researchers have already presented various methods for identifying sequence number assaults. In this study, a new technique and routing protocol is developed to proactively identify those attacks in MANET. This also helps to eliminate the false nodes in the network who are frequently misbehaving. The proposed SRD-AODV protocol includes secure neighbor node discovery for secure route discovery by selecting trusted node detection, hybrid cryptographic methods. This protocol also identifies suspicious nodes that launch attacks and isolates them from the network with a number of constraints in order to stop them from routing. The popular open-source Network Simulator is used in simulations. The SRD-AODV protocol also compares with AODV, EDRI -AODV protocols [11]. The proposed SRD-AODV routing protocol can guarantee that data packets travel through network with maximum security. In a malicious environment, it provides essential security fundamentals including authentication, non-repudiation, confidentiality, and integrity. This SRD- AODV protocol guarantees that only legitimate nodes can participate and also achieves access control over the participants by distributing authentication keys before routing process begins.

The focus of this study is on developing a better method for building algorithms for securing MANET from sequential attacks.

- To establish secure route from secure node discovery, which protects from sequential attacks. The network is self configurable and it secures nodes at the time route discovery and neighbor discovery process.
- To detect and prevent malicious nodes.
- To focus high mobility networks.
- To achieve maximum authentication against sequential attacks by providing secure neighbor and route discovery, cryptography and incursion detection process.

2 Methodology

The secure data transmission against sequential attacks in MANET is proposed with several process and components. The node authentication initially performed at the time of node initialization with a set of private and public keys. After node initialization, the secure neighbor will be identified at the time of route request. RREQ will be sent to the neighbor only who is already authenticated by the network. The detailed process of every component is explained below.

Node Authentication: It is the process of authenticating mobile nodes and later every node will be verified for secure transmission. This validates the nodes by its identity. Due to limited network resources in MANET, it is important to design an effective method for node authentication. The proposed SRD-AODV performs node authentication in on demand scenario. For secure key generation and sharing "Elliptic-curve Diffie–Hellman (ECDH) algorithm" is used. The ECDHA algorithm provides better key generation and secure key exchange over MANET. ECDHA is suitable for high dynamic mobile applications due to

its less computing power compared with RSA. ECDHA is based on private and public key pairs.

Secure Neighbor discovery and route establishment: The secure node discovery process selects the best neighbor node, who has least chances to be a malicious node in the network. So, initially five steps is performed to detect secure neighbor.

To enhance performance of secure routing protocol the major security components are used and mentioned in Figure 1 .

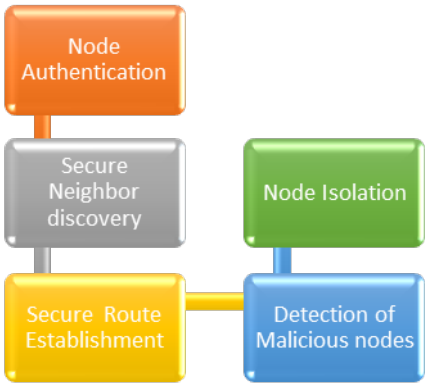

Fig 1. Security components of proposed work

1] Implementing elliptic-curve Diffie-Hellman (ECDH), a protocol for anonymous key exchange that permits network links, each of which is equipped with a set of public and private elliptic-curve keys. A secret key is produced and transmitted across an unsecured channel by employing this node. Here for each node in the transaction region a pair of public key and private key generated. The key generation process is done with the following equation 1.

$$ki = \sum_{i=0}^{n} \left(\frac{n}{k}\right) Keygen(Pri^{k} + Pub^{k}) \tag{1}$$

Here, ki is Key generation process of each node I, n is the total number of active nodes in the region, Pri^{K} is the private key, Pub^{k} is the public key. From the private and public key pairs, the anonymous key is generated.

2] After generating an anonymous key pair for each node. Then source node broadcast a packet request, which is called as handshaking process. The initial HELLO packet is send to its neighbor along with its public key. Here the ECDH provides an anonymous key exchange in handshaking process also.

$$S = \sum_{i=0}^{n} \left(\frac{n}{k}\right) Broadcast(ki + Pub^{k}) \tag{2}$$

Here, S is the source node, which broadcasts the request packet to all neighbors with the anonymous key ki and its public key Pub^{k}.

3] After receiving request packet from S, it verifies the key and adds that node as a neighbor with its public key along with its time value. The equation 3 shows the verification process done at receiver side R. Here T is the time value.

$$R = Verify(ki,\ Pub^{k}, T) \tag{3}$$

4] Each mobile node in the specific region responds to the greeting message and transmits the ID in addition. From this, a trust node list is generated.

$$ReceiverReply(ki,\ Pub^{k}, T) - \rightarrow S \tag{4}$$

5] If the received packet contains timestamp value, then it will send RREQ to that. The replies are valid for a particular time window. After that, source node self-authenticates to each of its first hop neighbors by fetching the reply that it received from them and adds them into the expected trusted neighbor list.

$$ND = validate\ (Reply\ (ni))\ \ add\ to\ \ (TNL) \tag{5}$$

Here ND, is neighbor node discovery process, which validate and add from the reply received from every node. The secure anonymous key is hided in the reply packet. If the validation is successful, then the node with its anonymous

After completion of the secure neighbor discovery phase the route is discovered by adding the link between nodes. For example, from the network, the route will be S1 $\rightarrow$ 2 $\rightarrow$ 3 $\rightarrow$ 4..... $\rightarrow$ D11. This process is a proactive manner, if the valid node acts as a vulnerable part, then our reactive incursion detection system helps to find and eliminate the node in the network for a particular period of time.

Node Isolation system: Design of incursion detection system in the proposed work can able to detect malicious activity especially sequential attacks and isolates the misbehaving node for a particular time period. There are so many techniques have used in the literature to detect and eliminate the malicious node. However, the proposed work contains different score based isolation process to ease the network transactions.

Here the anonymous key is used to identify the frequent, infrequent and rare malicious behaving nodes. The rest of the nodes can get the information about their neighbor in easy manner. After detecting malicious nodes and their activities the node can be classified into malicious or legitimate. This result category will be added to the data packet at the time of RREP, so the protocol can select best route from the RREP and the value over on it. The secure routing mechanism should be proactive, but in MANET, the proactive process is not always possible. So the proposed system works in both proactive and reactive manner. In this way pre-path security is achieved in SRD-AODV protocol. SRD- AODV routing protocol provides assurance that such malicious node should not able to join the network and providing hazards to other nodes or route.

3 Results and Discussion

In the simulation and experiments, the NS-2 simulator is used. Ns-2 is widely used network simulator and results are obtained from that for comparison. In order to prove that the SRD-AODV protocol gives better performance compared to the AODV and other EDRI based approaches, we compare the performance of those approaches with different QOS (quality of Service) metrics. For the experimental process, different simulation parameters have used for totally 300 seconds simulation. The simulation area topography is generated with 1000 m$\times$1000 m. The performance of SRD-AODV protocol is compared with the traditional AODV protocol and improved AODV with EDRI. The different parameter-based performance comparison of various techniques is explained. This includes packet delivery ratio, throughput, and delay and energy consumption.

The number of mobile users in the simulation is 150 the metrics end-to-end delay, packet delivery ratio, average packet drop and throughput are measured.

3.1 Simulation Results

Delay: - Delay is calculated by taking difference between the time when first packet was transmitted by source and time when first packet successfully reached to destination.

$$Delay = Received\ Packet\ Time\ \ Send\ Packet\ Time \tag{6}$$

Packet Delivery Ratio: It is determined by dividing the total number of packets that were successfully acquired by the total number of packets transmitted by CBR sources.

$$Packet\ Delivery\ Ratio = \frac{Total\ Packets\ Received}{Total\ Packets\ Sent} \tag{7}$$

This metric gives how secure routing protocol works securely and efficiently.

End-to-end delay is calculated by subtracting the time of packet generation from the time of packet receiving at the destination. The time it takes to generate a packet is subtracted from the amount of time it takes for that packet to be received at its final destination in order to arrive at the end-to-end delay. Figure 2 presents a comparison of the performance of the existing AODV protocol, the EDRI-AODV protocol, and the proposed SRD-AODV protocol in terms of the total end-to-end delay value. In this section, the delay value for each protocol is determined, and then it is compared to the proposed system. From the results it is observed that the proposed SRD-AODV algorithm achieves 58.5% less E2E delay than AODV and 44.5% less than EDRI-AODV.

Figure 2 presents a comparison of the total end-to-end delay for each of the methods with the delay that would be incurred by the proposed system. It is the total amount of time that occurred during the data transmission from the source to the destination after the attack verification was completed without any problems utilising the modified protocol. When there are more than 100 mobile nodes, overhead occurs, which results in an increase in delay. This happens when the number of mobile nodes is

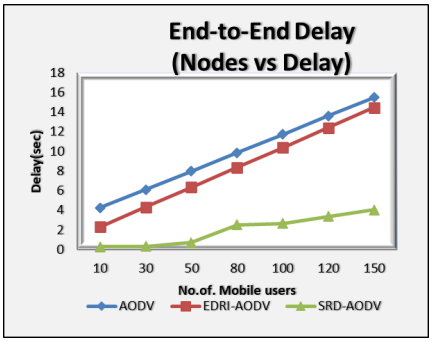

Fig 2. Delay for varying the mobile users

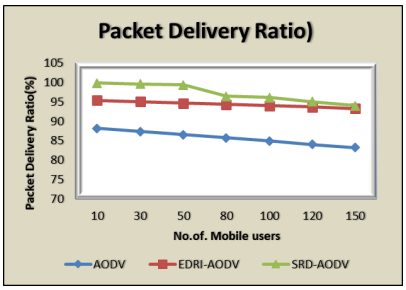

Fig 3. Packet Delivery Ratio

greater than 100. When compared to the AODV protocol, the use of ECDH and region-based verification in AODV results in a delay reduction of around 85 percent.

Figure 3 shows that the PDR increased as the source discovered more numerous routes; hence, an increase in the number of mobile users will decrease the PDR. However, SRD-AODV has a PDR that is greater by 4.92% than EDRI-AODV and 12.23% than AODV because it excludes network attacks, has flawless routes, and prevents packets drop or connections fail. This is because SRD-AODV has more perfect routes.

Table 1. Comparison of existing algorithms for Secure Routing Protocols for MANET

Authors	Model Descriptions	Results
Tri Kuntoro Priyambodo et al. (2021) [5]	AODV and DSDV protocols are analyzed.	PDR of AODV is between 0.980403-1.00 and between 0.006536-0.006668 throughput. AODV is better than DSDV
Prabha et al. (2022) [6]	Hybrid Bat (HBAT) is to enhanced the AOMDV with Hybrid Bat is optimizes the routing.	HBAT achieved 7.8% minimum E2E delay and achieved 55% greater throughput.
Ali Abdulmalek et al. (2022) [12]	Improved AODV routing protocol	Improved AODV achieved 53% PDR and 1.27% E2E delay.
Abdul Majid et al. (2022) [7]	A hybrid AODV for route discovery mechanism and minimum link breakage using hybrid AODV.	Hybrid AODV achieved 5.77% E2E delay and 213.5kbps throughput.
Proposed SRD-AODV	The proposed SRD-AODV protocol uses a variety of elements and techniques to establish efficient authentication using Elliptic Curve Diffie-Hellman algorithm (ECDHA) techniques, offering both proactive and reactive solutions.	The proposed SRD-AODV protocol achieves 95.61% PDR and 1.642 % E2E delay.

4 Conclusion

Wireless technologies have grown in popularity because of their simple deployment, high mobility, and dynamic infrastructure. Numerous security problems are occurring in this network in a variety of ways and under various circumstances. This problem makes security for data packet routing a very challenging problem that requires a range of solutions. The novel feature of the proposed system is the development of a hybrid framework with secure neighbor discovery, node authentication using ECDHA, and malware detection and isolation mechanism in order to provide high security over MANET routing and security against sequential assaults. The AODV protocol is integrated with the hybrid framework and renamed as SRD-AODV. Security is offered in two phases of the SRD-AODV routing protocol, including security to route and security to data. First-stage evaluations of route and neighbor security include secure neighbor discovery, which can distinguish between real and fraudulent nodes. Non-legitimate nodes are prevented here by the SRD-AODV protocol before the routing process starts. In order to identify malicious nodes and prevent utilizing them in routing, AODV uses the best authentication system and a secure neighbor finding technique. The suggested approach enhances packet delivery and obtains good attack detection ratings. Results from the intended study included 150 mobile nodes. SRD-AODV achieves 58.5% less E2E latency than AODV and 44.5% less than EDRI-AODV while having a PDR that is higher by 4.92% than EDRI-AODV and 12.23% than AODV. The methods can be extended in the future with additional mobile nodes using various MANET protocols.

References

1) Alameri IA, Komarkova J. A Multi-Parameter Comparative Study of MANET Routing Protocols. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. 2020;p. 16. Available from: https://doi.org/10.23919/CISTI49556.2020.9141119.
2) Alkahtani SM, Alturki F. Performance Evaluation of Different Mobile Ad-hoc Network Routing Protocols in Difficult Situations. *International Journal of Advanced Computer Science and Applications*. 2021;12(1):12. Available from: https://doi.org/10.14569/IJACSA.2021.0120119.
3) Bhatia A, Kumar A, Jain A, Kumar A, Verma C, Illes Z, et al. Networked control system with MANET communication and AODV routing. 2022. Available from: https://doi.org/10.1016/j.heliyon.2022.e11678.
4) Van-Hau Hoai Nguyen, Nam V, Dao L, Khanh QV. An Improved Agent-Based AODV Routing Protocol for MANET. 2021. Available from: https://doi.org/10.4108/eai.23-6-2021.170241.
5) Priyambodo TK, Wijayanto D, Gitakarma MS. Performance Optimization of MANET Networks through Routing Protocol Analysis. *Computers*. 2021;10(1):2. Available from: https://doi.org/10.3390/computers10010002.
6) Prabha R. An Enhanced Ad hoc On-Demand Multipath Distance Vector Routing using Hybrid Bat Algorithm. *Research Square*. 2022. Available from: https://doi.org/10.21203/rs.3.rs-1097752/v1.
7) Soomro AM, Fudzee MFB, Hussain M, Saim HM. A Hybrid Routing Approach Comparison with AODV Protocol Regarding Speed for Disaster Management in MANET. *Journal of Computer Science*. 2022;18(3):204–213. Available from: https://doi.org/10.1088/1742-6596/2327/1/012057.
8) Shantaf AM, Kurnaz S, Mohammed AH. Performance Evaluation of Three Mobile Ad-hoc Network Routing Protocols in Different Environments. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2020;p. 1–6. Available from: https://doi.org/10.1109/HORA49412.2020.9152845.
9) Talib RHA, Alothman MSB, Mohammed. Malicious attacks modelling: a prevention approach for ad hoc network security. *Indonesian Journal of Electrical Engineering and Computer Science*. 2023;30(3). Available from: https://doi.org/10.11591/ijeecs.v30.i3.pp1856-1865.
10) Saleh SA, Zuhairi MF, Dao H. A Comparative Performance Analysis of Manet Routing Protocols in Various Propagation Loss Models Using NS3 Simulator. *Journal of Communications*. 2020;p. 537–544. Available from: https://doi.org/10.12720/jcm.15.6.537-544.
11) Srilakshmi U, Alghamdi SA, Vuyyuru VA, Veeraiah N, Alotaibi Y. A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. *IEEE Access*. 2022;10:14260–14269. Available from: https://doi//10.1109/ACCESS.2022.3144679.
12) Saif AAA, Kumar K. Enhance the performance of AODV routing protocol in mobile ad-hoc networks. *Journal of Physics: Conference Series*;2022. Available from: https://doi.org/10.1088/1742-6596/2327/1/012057.