Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

TRUST-BASED AOMDV PROTOCOL MULTIPATH ROUTING IN MOBILE ADHOC NETWORKS

S. Sekar[1], Assistant Professor, J. Guruswaminathan[2], M.Tech, Data Science
Department of Information Technology
SRM VALLIAMMAI ENGINEERING COLLEGE

Abstract

Each mobile node in a mobile ad hoc network (MANET) serves as both a gateway and a terminal. A dependable routing protocol is selected while acting as a router to make sure the packet finds its destination, and an agent is in charge of transmitting the packet while acting as a terminal. In this paper, we use the Ad Hoc On Demand Multipath Distance Vector (AOMDV) routing algorithm to implement secure packet transmission in mobile ad hoc networks (MANET). Although not completely immune to attacks, the multipath extension of the AODV (Ad Hoc On Demand Distance Vector) routing protocol, AOMDV, is more dependable than its parent protocol. The primary goal is to keep the packets secure in a hostile environment with numerous attackers. To protect the packets from black-hole assault, elliptic curve cryptography (ECC) has been used. Compared to other public-key encryption, elliptic curve cryptography offers security with a smaller key size. Using NS-2.35, a discrete event network simulator, we set up three different kinds of environments: a secure one without malicious activity, a hostile one with black-hole attackers, and one with ECC implementation by the agent. We then analysed the performance of each environment.

KEYWORD: MANET, AOMDV, Elliptic Curve Cryptography (ECC), Black Hole attack.

1. Introduction

A Mobile Ad-hoc Network (MANET) is a grouping of separate mobile nodes that interact with one another by establishing a multi-hop radio network in an area devoid of infrastructure. In MANETs, nodes act asboth servers and terminals. Furthermore,unlike wired networks, ad-hoc networks' routing paths are dynamic in character. As a result, some security measures made for connected topologies cannot be used with ad-hoc networks.

As a result of their adaptability, mobilenodes frequently change their topology, which makes it challenging to develop safe ad-hoc routing protocols. Each node within a node's straight transmission range receives the data that a node transmits. A MANET [1] routing protocol will be more susceptible to various types of malicious assaults if the ad-hoc network is unsecure in some way. The majority of the routing protocols suggested for MANETs presume a reliable and trustworthy environment and do not initially design for security concerns. It looked into the AOMDV protocol's security in this system. AOMDV is a multipath version of the AODV routing protocol that protects against black-hole attacks.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

2. Related Work

Adhoc routing protocols in use are vulnerable to several attacks that could allow the attacker nodes to influence path selection or launch denial-of-service attacks. We specifically used the blackhole attack, in which malicious nodes draw packets and prevent them from getting to their intended location. In this attack, the hostile node draws packets but does not send any of them to the target, dropping them all instead. The packets sent by the nodes are not delivered to the intended location as a result of this assault. Although not entirely immune to attacks, the multipath extension of the AODV (Adhoc On Demand Distance Vector) routing protocol, AOMDV, is moredependable than its parent protocol. Theprimary goal is to keep the packets secure in a hostile environment with numerous attackers. To protect the packets from blackhole assault, elliptic curve cryptography (ECC) has been used. An intrusion detection system (IDS) schemethat uses a hop count mechanism toidentify the attacker is suggested as a defence against black hole attacks and to secure AOMDV routing in MANET.

3. Proposed work

The sequence of steps in Fig. 1 illustrates aprocess for protecting a data packet in the mobile adhoc network against a black hole assault. Establishes the topology first, then finds all possible routes between the source and the target, as shown in the figure. The AOMDV algorithm will be used for path selection. Multiple routes between source and target are discovered by the protocol. The other route will be used right away for data transmission if any method fails. The keys are spread among the MANET's legitimate nodes using ECC. Both the public and secret keys will be used to encrypt and decrypt the data.

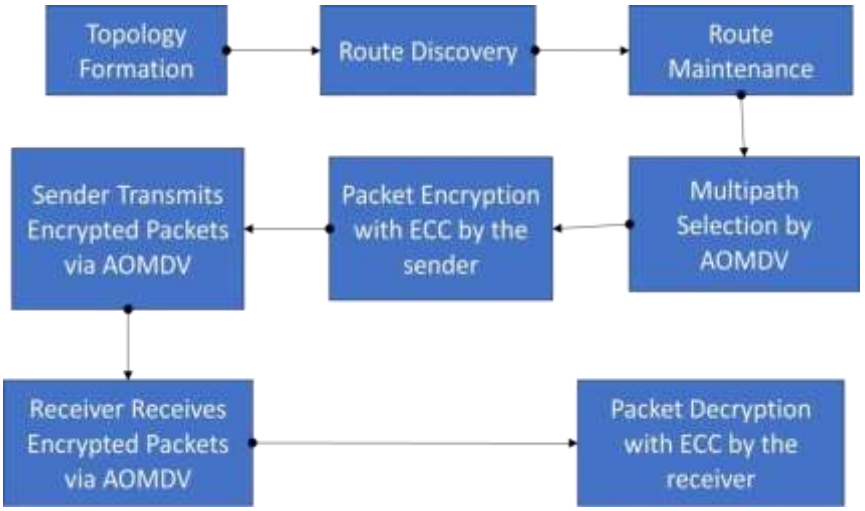

Figure 1: Block diagram

As a result, data will be safely transmitted between each node in thenetwork and each node will be aware of allother nodes. Without the shared secret key,the malicious node will not be able to decrypt the encrypted data even after an assault.

3.1 Benefits

Smaller routes are unlikely to benefitmuch from local repair, but bigger routes, particularly those with 10 or more hops, greatly benefit from local repair. This is due to the increased likelihood of link breaks on longer routes. If the intermediary nodes continuously transmit Route Error messages to the source, which in turn continuously initiates Route Discovery, a large number of control messages are consumed, and performance suffers. This is accomplished by revoking route discovery whenever any route has fewer than two paths, as opposed to the original AOMDV, which only revokes route discovery when there is no path to the destination. By using this new rule, a backup path can be created while the main route is still operational. Following the previous route discovery process, new nodes that joined the transmitting rangecould be regarded as new neighbours and could participate in the search for new paths.

4. Module Description

4.1 Node Formation

As a result of their adaptability, mobilenodes frequently change their topology, which makes it challenging to develop safe ad hoc routing protocols. Each node within a node's straight transmission rangereceives the data that a node transmits. A MANET [1] routing protocol will be more susceptible to various types of malicious assaults if the ad hoc network is unsecure in some way. This proposed method produces a maximum throughput of 0.85 bits per second, a maximum detection rate of 91 percent, and a maximum packet delivery ratio of 89 percent with a minimum energy requirement of 0.10 mjoules and a minimal delay time of 0.004 msec. The selective packet dropping attackwas used to test the proposed strategy.

4.2 Multipath Selection

The simulation study demonstrates that the AODV Multipath protocol performs better in low mobility and higher node density scenarios, while the AOMDV protocol works best in high mobility scenarios. SMR operates most effectively in networks with few nodes, but as density rises, the protocol's efficiency deteriorates. As an extension of AODV, AOMDV offers numerous paths. Each RREQ andcorresponding RREP in AOMDV specifiesa different route to the source ordestination. Each node maintains multiple routes in its routing entries. For each destination, the routing entries include a list of next-hops and the associated hop counts.

4.3 Encrypted Packets Transferred

To protect the packets from blackhole assault, elliptic curve cryptography (ECC) has been used. Compared to other public-key encryption, elliptic curve cryptography offers security

with a smaller key size. Using NS-2.35, a discrete event network simulator, it set up three different kinds of environments: a safe one without malicious activity, a hostile one with blackhole attackers, and one with ECC implementation by the agent and analyzed.

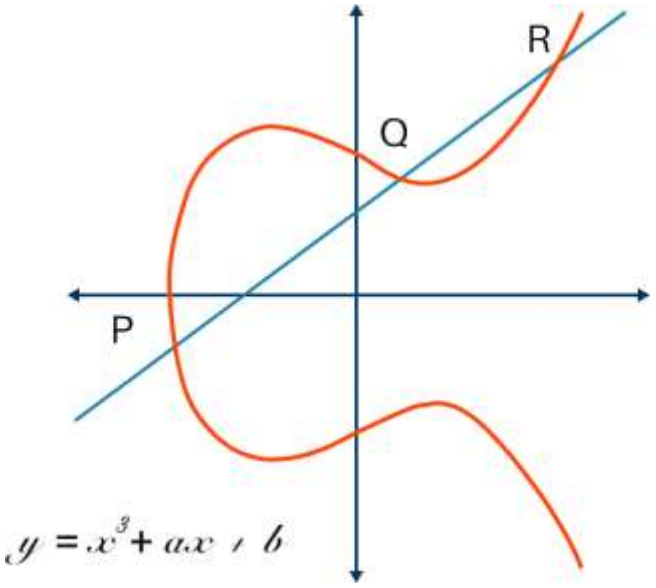

Figure 2: ECC Curve

4.4. Detection of Malicious Node

In a square area measuring 1000 x 300meters, it takes into account 4 network sizes with 30, 50, 70, and 100 nodes. To evaluate the protocol performance for low and high node density, we change the number of nodes. 10 or 20 CBR/UDP connections, with a sending rate of 4 packets per second between arbitrarily selected source and destination pairs, are used to analyse traffic patterns. Throughout the simulations, connections occur at random times. For the various routing algorithms, we employ the sametraffic and mobility patterns. Results from simulations are the averages of 20 situations with various seeds. The network interface queue capacity for routing anddata packets is always set to 64 packets, and data packets have a fixed size of 512 bytes.

5. C-means Algorithm

Density peak served as the foundation for an improved C-means algorithm method, and cluster heads (CHs) were selected in a foreseen way based on recent, indirect, anddirect trust. The calculation is based on thevalue of nodes that are additionally locatedat the trust level. Even CHs participate in the alternate pathways, and the optimal route is selected by combining the various paths from these Cluster Heads based on the predicted hybrid protocol and the aggregate characteristics of the optimum route, such as throughput, latency, and connection.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

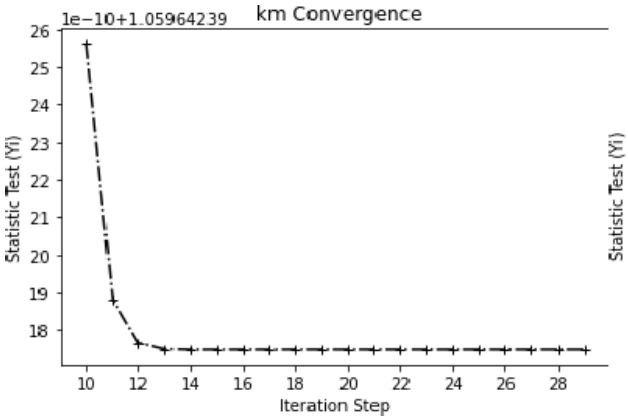

Figure 3: KM Convergence

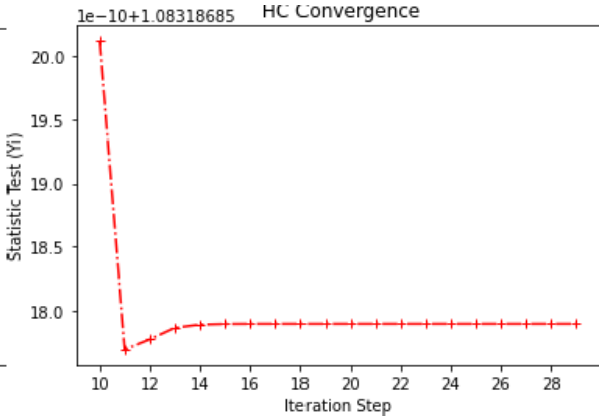

Figure 4: HC Convergence

Designing reliable routing algorithms that can adjust to the frequently changing network topology and offer a variety of alternative routes from source to target is one of the major challenges faced by Wireless Mesh Networks. When the active path fails, data can still be transmitted overalternative paths thanks to the various Multipath routing protocols that have beensuggested. One of the most popular reactive algorithms for multipath routingin wireless mesh networks is the Ad hoc On Demand Multipath Distance Vector (AOMDV) Routing Protocol.

6. Methodology

The key to the AOMDV protocol isassuring that the multiple paths are disjoint and without loops. The mechanism that keeps the route discovery current is dependent on flooding. Every node has AOMDV path update rules in place to preserve loop-freeness and disjointness.

The following characteristics are upheldby the AOMDV protocol: [1]Keepsseveral loop-free paths active based on the stated hop count. maintains a node- or link-disjoint route. Processes each RREQ packet in order to keep numerous paths open. [4] maintains a new route by selecting a routing path while taking the highest sequence number into account. [5] If the sequence number is the same, take into account the minimal hop count. We achieve the same outcomes with multi-path routing as we do when data flows through a single router. It compare the results after applying TRW to the data on each router for discovery. In this instance, we discovered that their method produced a lot of false positives or negatives.

It can build up a link path multicommodity network flow optimization model for an appropriate traffic engineering goal by using the models, given that there are multiple paths connecting any two hosts. By taking into account the optimisation model for traffic between edge switches, the model can be made somewhat compact because hosts are linked to edge switches. Mobile adhoc networks have nodes thatcan be tricked into acting as an adversary. So transmitting encrypted data packets is problematic. A public key cryptographic method

called elliptic curve cryptography (ECC) offers the same level of protection as other public key cryptography but with smaller key sizes. The formation and upkeep of the network are challenging due to these frequent changes in the network topologies.

8. Implementation

The different facets of the AOMDV procedure. It notes that AOMDV provides a sizable delay decrease. In a variety of mobility and traffic situations, AOMDV consistently provides a better overall routing performance than AODV and other routing protocols. The mobility of nodes is the primary causeof shifts in topology. While nodes in WMNs are allowed to move around, when a topology change occurs in the network, other nodes must be informed in order for outdated topology information to be updated or removed. It is presently developing a productive AOMDV protocol. After examining the various facets of AOMDV, we have come to the conclusion that while AOMDV has many benefits, there are some areas that still require improvement. Based on the aforementioned results, we draw the conclusion that the multi-path routing protocol's link disjoint path option outperforms its single-path or node disjoint path options in terms of total performance. In comparison to AOMDV, AODV, TORA, DSR, and DSDV protocols, the results will be obtained as modified AOMDV, which offers superior performance.

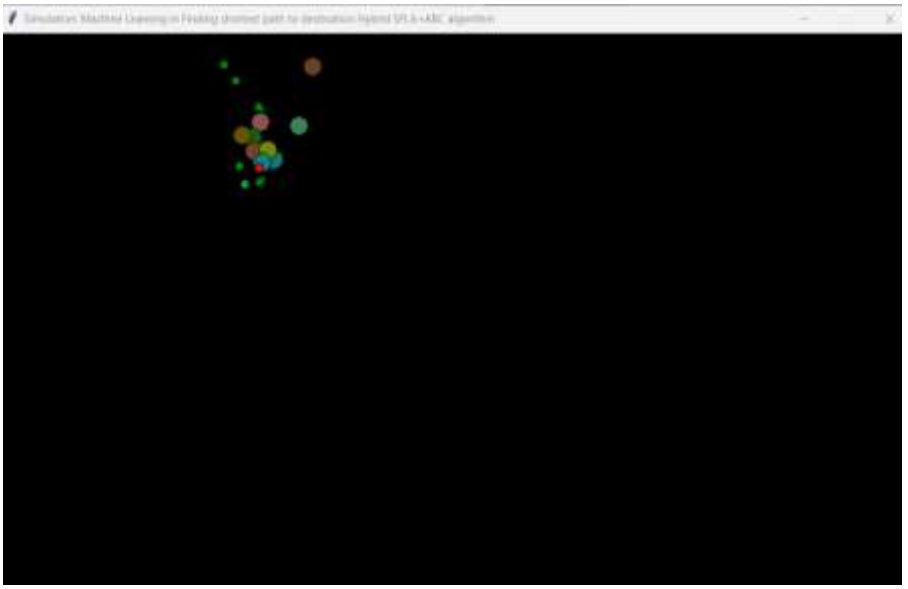

Figure 5: Simulation Result

9. Result

Existing ad hoc routing protocols are vulnerable to several attacks that could allow the attacking nodes to influence the route selection or initialize denial-of-service attack. We specifically used the blackhole attack, in which malicious nodes draw packets and prevent them from getting to their intended location.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

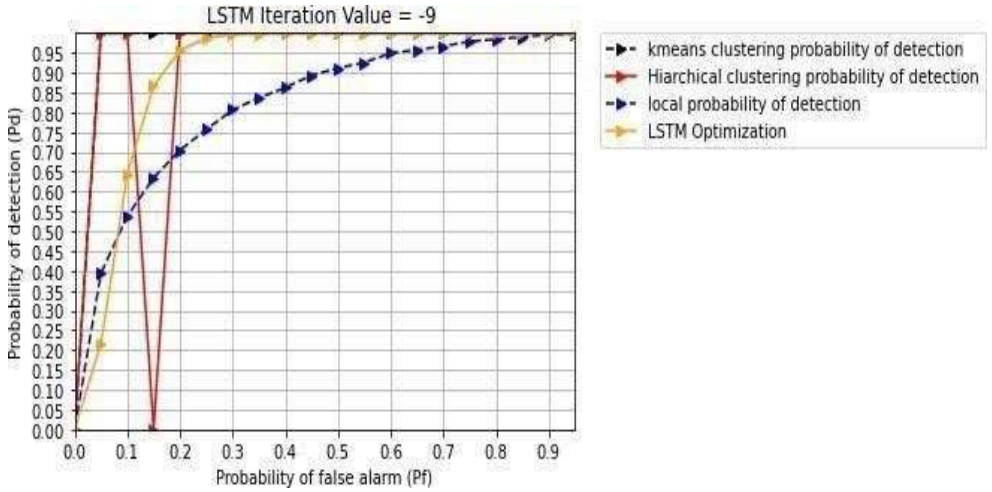

Figure 6: LSTM Result

The efficacy of this suggested technique against other attacks can be evaluated using other attacks. The protocol, whichcombines AOMDV and ECC, offers a wayto secure messages in the hostile MANET environment. To identify and steer clear of malicious networks, this technique can be used in conjunction with an intrusiondetection system (IDS).

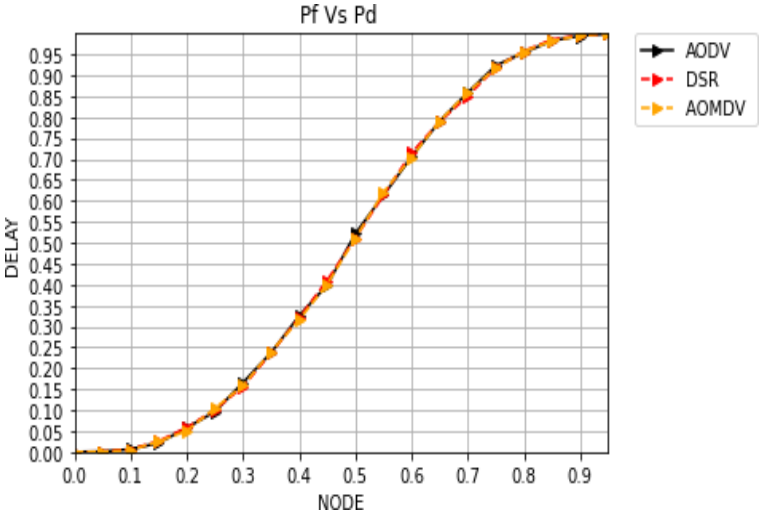

Figure 7: Performance Result

10. Future Work

The suggested modified AOMDV protocolwith local repair process, or AOMDV-LR, is used in this system. More data packets arrive at their target thanks to local repair. As the network grows, the length of these routes' paths also lengthens. When no other option is available, AODMV-LR initiates local repair at all the preceding nodes of failure that are closer to the destination than the source, i.e., not just the precursor node participates in local repair but all the preceding nodes as well. As a result, routes are expected to be repaired quickly and with minimal overhead.

REFERENCE

[1] Arora Vandana, Ahuja Sunil “Trusted keymanagement with RSA based security policy for MANETs”, International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454-132X, (Volume2, and Issue3).

[2] Bansal Priyanka, Gupta Anuj K., “Impact of black hole and neighbor attack on AOMDV routing protocol”, International Journal of Innovations in Engineering and Technology (IJIET), Vol. 3.

[3] Marina, Mahesh K., and Samir R. Das. "Ad hoc onǦdemand multipath distance vector routing." Wireless communicationsand mobile computing 6.7 (2006): 969-988.

[4] Raju M Janardhana, Subbaiah P., Ramesh V., “A novel elliptic curve cryptography based AODV for mobile ad-hoc networks for enhanced security”, Journal of Theoretical and Applied Information Technology, December 2013.

[5] Shrivastava Sonal, Chetan Agrawal, andAnurag Jain. "An IDS scheme against black hole attack to secure AOMDVrouting in MANET." arXiv preprint arXiv:1502.04801 ,2015.