Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhanced Security in MANETs Using AODV Protocol and Detection Algorithms

Neelam[1], Amit Sharma[2]*Lakshmi Shanker Singh[3]
[1-3]Assistant Professor, Deptt. of Information Technology, C.C.S. University Campus, Meerut.
[2]Assistant Professor,Deptt. of Computer Science & Engineering, C.C.S. University Campus, Meerut
(*Corresponding Author)

Abstract
This study introduces a brand-new security technique for MANETs to use with the AODV (Adhoc On-demand Distance Vector) routing protocol in order to improve its security and performance when under attack like explicit packet dropping (EPDA) and implicit packet dropping (IPDA). The first version of the AODV routing protocol did not include any safeguards. As a result, it can't stop any cyberattacks of any kind. However, AODV is safe due to the availability of numerous security methods. The technology that identifies them also provides a network-based strategy for minimizing the number of attackers. More investigation into this field, however, revealed a critical vulnerability in all currently available safe routing systems. Thus, existing security measures are resource-heavy and call for a sophisticated key-management infrastructure. In this paper, we describe a new way to protect the AODV routing protocol that combines digital signature and hash chain. This method can protect itself from hostile and unauthenticated nodes with little effect on performance.
Keywords: AODV, EPDA Attack, IPDA Attack, MANET.

1. Introduction

This type of wireless network, also known as MANETs or ad hoc networks, is made up of mobile devices and can be configured in various ways depending on the situation. There are several MANET nodes; join or exit the network at any time is completely up to them as a result, the network's topology will be constantly changing [1]. The mobile nodes will be able to communicate with each other if their wireless ranges are close enough to each other. A lack of communication will eventually lead to the two of them breaking up [2]. Other nodes will need to work together in order to communicate via wireless links that are too far away. The term "multi-hop network" is used in the computer networking community to describe this type of network [3]. Nodes in a MANET are required to serve as both hosts and routers because there is no infrastructure or centralized point of control. With several hops, different router nodes are responsible for ensuring the routing path is always correct [4]. So that they can work together effectively, they need an established method for directing communications. Network users have to work on MANET's routing technology because it simplifies network installation and can be completed in a short period of time. MANET is no different from any other network in terms of vulnerability to intrusion. In reality, a wireless network attack is far more likely than a wired network attack [5]. Hostile MANET threats include eavesdropping, spoofing, tampering with control packets, and denial of service. Denial of service is another example of this, when it comes to MANET's various network topologies, it uses both proactive and reactive routing technologies. The Ad hoc On-demand Distance Vector (AODV) routing protocol can be implemented immediately in an ad hoc network. As a result, dangerous attacks like the black hole attack are impossible to discover. As one of the most common AODV routing protocols, the black hole attack is one of the most common ways to break it. A malicious node sends routing control messages with a false sequence number attached, making it appear as though it had the shortest and most current path to the target. What the system entails in its entirety is in the event that a Black hole node has been compromised, it can be used for a variety of nefarious reasons, including denial

of service attacks and spoofing [6]. Security was not a consideration when the AODV protocol was first designed. It has been argued that AODV's route-finding algorithm has flaws AODV's route-finding mechanisms are examined, and a new technique for protecting the protocol from black hole attacks is offered in this paper. The AODV-based MANET under attack from the Black Hole was safeguarded in a variety of methods. The recvReply() function has been suggested as an option to safeguard the route update process. If this change is done, the current AODV route finding system will be improved upon. ERDA is the abbreviation for the present strategy that is being debated (Enhanced Route Discovery AODV). It was claimed in Section 4 of this research that our suggested technique lowered the amount of time needed to complete the AODV protocol while simultaneously introducing the least number of adjustments feasible. The AODV routing protocol and the MANET message format are discussed in detail in Sections 2 and 3 of this paper. After the Introduction, you'll find these sections. In addition, we'll go over how to administer routes, forward data, and identify new routes.

A denial-of-service attack can be carried out in a number of different ways, and we'll cover both of these methods in this section of the guide. In Section 5, we examine the different approaches that can be utilized to locate EPDA and IPDA assaults. There are graphs in Section 6 that show the simulation's outcomes. Section 7 focuses on the author's conclusion and future plans, which are explored in greater detail.

2. Ad Hoc On Demand Vector Routing

When these conditions are met, the AODV routing algorithm is classified as dynamically reactive. A dynamic routing system will choose the best route based on demand (upon request by a source node). Figure 1 depicts the steps that must be followed. There are a number of steps involved in determining the shortest path to the destination node. Two essential control signals are required for AODV to work properly [7]. The following are the details:

"RREQ" means Route Response and Request (RREP). Both control messages contain the "target sequence number." This number shows how recently a route has been traveled. The Occurrence of the Path Process Uncovery Sending control packets and RREQ messages to nearby nodes A, B, and C helps the source node S find the fastest path to the destination node D. A node can respond to an RREQ message in several ways.

A. Respond with an RREP message if the receiving node is the destination or an intermediate node with recent route information.
B. After getting to the destination node or an intermediate node, update the routing table item for the reverse path.

If an intermediate node's routing table destination sequence number is greater than or equal to the RREQ message, it has "fresh enough routes" to the destination node (with fewer hops).

3. Literature Survey

Ad-Hoc On-demand Distance Vector Routing (AODV) In the AODV system, new routes are found as needed. Both DSDV routes and AODV routing use the same sequence numbering method, so they are similar in a number of ways [8]. Hop counts and DSR are used to get rid of network loops. Sequence numbers are used to figure out how new the information is. These routes are made to reduce the number of hops and find new routes on routes that don't get as much traffic [9].

Route discovery If an entry is found in the source node's routing table, it must be legitimate and active in order for the data to be sent. Routing table items that are not in the routing table are discovered by broadcasting RREQ messages throughout the network. The RREQ contains the following fields:

<source _addr, source_ sequence_#, broadcast_ id, dest_ addr, dest_ sequence_#, hop _cnt>

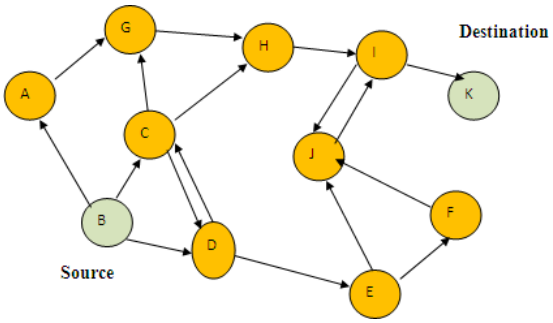


Fig 1 AODV Route Discovery (Propagation of RREQ)

RREQs each have their own set of broadcast ids and source _addrs. Each time the source sends a new RREQ, the broadcast_id is incremented. If the RREQ is received by a neighbouring node, A shorter TTL and a higher hop count are used to rebroadcast the received RREQ if it's not a duplicate. Here, RREQs that are no longer needed are disposed of.

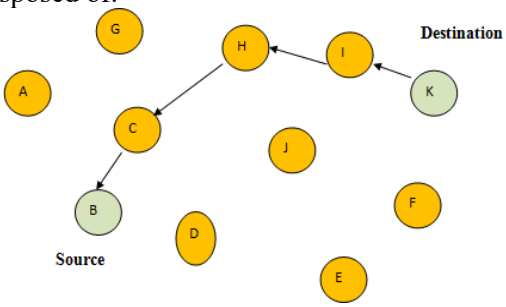


Fig 2 AODV Route Discovery (Propagation of RREP)

An intermediary node that has a route to the destination responds to the RREQ with a route response message (RREP) as shown in figure 2. Forwarded routes are built by sending the RREP in Unicast from the destination node to the source node [10].

Data Forwarding: Data is transmitted along a path after finding its end node. The source transfers the data packet to the next hop. It's connected to the final node. Before proceeding, this hop checks its routing database. The data packet is sent to its next hop. Each node's transmission can affect how long a route takes to send a data packet. After the maximum number of retransmission attempts, a node sends an error message to the next hop [11].

Route maintenance: One method for retaining routing information in a MANET is based on link layer acknowledgement, and the other method is based on repeated HELLO messages. Both of these methods are considered separate link-checking processes. HELLO messages are sent at regular intervals to the neighbours on the hop that follows in order to verify connectivity with them [12]. When a node in a network does not receive a HELLO message from any of its neighbours within a certain amount of time, the node considers the connection between itself and its neighbours severed. If a node is unable to receive MAC layer acknowledgments after sending the data packet the maximum number of times, then the link is regarded as broken. An AODV-provided local route repair procedure and RERR notifications are the two means by which a broken route can be addressed [13]. The intermediate node, from where the route is broken for the subsequent hop towards the destination, will seek to locate an alternate path by utilising a route discovery process that will take it from itself all the way to the destination. When a source node sends an RERR message as shown in figure 3, it makes the currently established route invalid and starts a new route-discovery process at the destination node [14].

As a result of its reactive nature, AODV generates the least amount of routing overhead in networks that are both underutilised and congested. To find the best path, AODV avoids crowded locations and recommends routes with the fewest hops possible.

Terminology used with respect of AODV
Broadcasting: Because MANET is a wireless network, every node in the network can receive any packet that is transmitted into the network, whether it is a control or data packet. Every node process and receives broadcast packets, but the term "broadcast packets" only refers to those that have a broadcast destination address in their destination field [15].
Forwarding node: When the packet must still be sent to the destination node, it is sent to a forwarding node. A forwarding node is an unintended recipient or source of data or control.

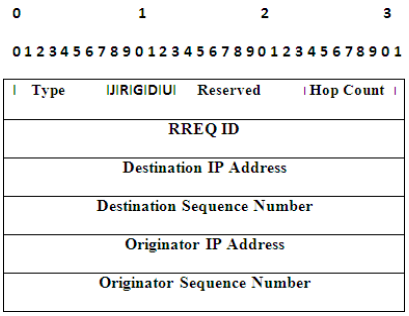


Fig. 3 Route Request message format Type-1

Forward route: The route used for data transmission from a source node to destination nodes is known as the forward route.
Invalid route: The AODV protocol will mark as invalid any routes that have been used for data transmission in the past but have not been utilized for some time. Because of this process, these routes will be taken out of the routing database at some point in the future[15], [16].
Active route: A route that is always used to send data and whose lifetime is always updated because of this is called an "Active route."
Reverse route: The RREQ travels backwards from source to destination. A route connects source and destination nodes.
Sequence number: This number is updated by each RREQ or RREP source node. Other nodes in AODV routing protocol messages use it to assess control packets' freshness.
MessageFormatinAODV
RouteRequest(RREQ)MessageFormat
G: RREP flag that is no longer used
D: Only-destination flag
U: sequencenumber which is not known
Reserved: Zero Counted
Hopcount: how many hops it traveled from the origin IP to the processing node.
RouteReply(RREP) Message Format is shown in figure 4 and Route Error Message Format in shown in figure 5.

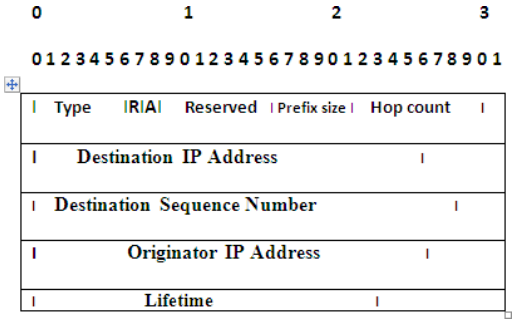


Fig 4 Message Format Route Reply Type-2

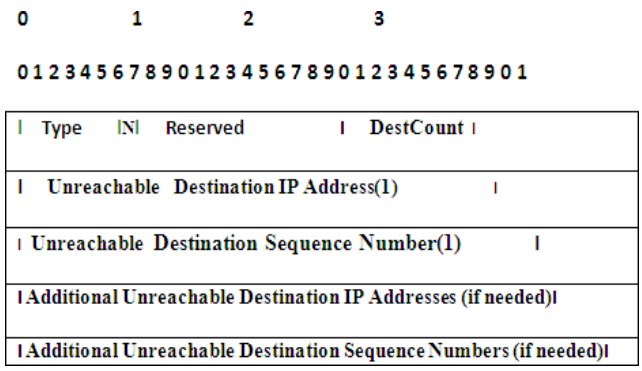


Fig 5 Route Error Message Format

J: Joinflag
R: Repairflag
N: delete Flag is not Zero
Reserved: received as Zero
Destination Count: not received destinations counted inthe text; should be beatleast1.

Unreachable Destination IP Address is a destination's IP address after a link failure. The unreachable destination's sequence number is the preceding unreachable destination's IP address.

4. Denial of Service Attack

Attackers drop explicit packets (EPDA) is when a source node's network purposefully drops data packets. The source node sends an RREQ message if the destination node has no route in the routing database. RREQ broadcast messages contain source _addr, source _sequence no, broadcast id, dest _addr, dest _sequence no, and hop _cnt>. RREQs can't share the same broadcast ID and source address. When the source broadcasts more RREQs, the broadcast id grows. Nodes that receive RREQs from other nodes use the SEEN TABLE to find database duplicates. Lowering the TTL and increasing the hop count rebroadcasts a non-duplicate RREQ into the network. The network administrator must approve this. A redundant receiver/expansion unit sends no signals (RREQ). An intermediate node sends an RREP message to the source node when it finds a new path to the destination. RREP message generation Checking the destination sequence number in an RREQ message shows how recently a route was utilized [16]–[21]. If the node has a route with a greater sequence number than the RREQ message, it can send an RREP message. If no intermediate nodes have discovered a new route for the destination, the destination responds with the route reply message (RREP). When the RREP arrives at the source node from the destination, the forward route is created. Using AODV's route discovery technique, the attacker node will become an intermediary for the targeted data transmission line.

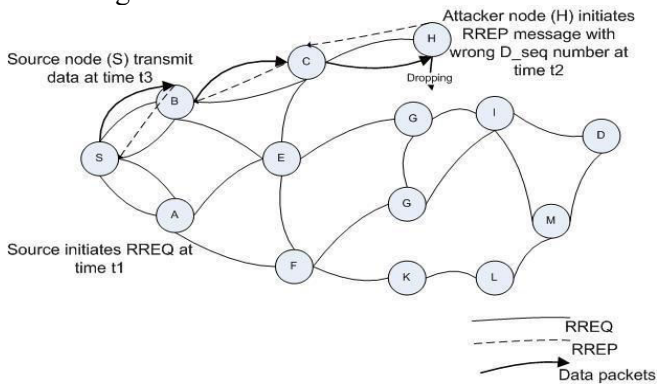


Fig. 6 Explicit Packet Dropping during Route Discovery

Once it receives the source node's broadcast message, it will start generating a better target sequence number. This message will be delivered at the originating node. The source node can't identify fake RREP messages sent by the attacker node. Changing a node's routing database sends data. The source node ignores RREP messages. This is true whether messages come from the recipient or another node. Instead of transferring data along an active route, it joins it and discards incoming packets. This figure shows the earlier described attack technique (Fig. 6). The H node symbolises the assailant, whereas S represents the assault's origin. t1 arrives first, followed by t2 and t3. Figure 4 details the packet drop assault. In this attack, the attacking nodes will operate independently, ignoring other nodes' messages. As long as he's not in a data communication channel, the attacker won't block network data. This kind of attack just makes it hard for the network to pass on data packets, making it hard to find the attacker node. Figure 6 shows the source and destination nodes (D), At t1, node S begins route discovery and node G receives the RREQ. Node G's routing database has a new route for node D. Node D will respond to G's RREP request. RREP identifies the information's source. Node G received this node's unicast RREQ message. Node E will deliver the RREP message because node G sent it. Once malicious node S sends an RREP message and data, malicious node E receives all data packets on the allocated path. Node E receives unneeded data packets. Node E's transfer between S and D didn't alter its operation (see Figure 4). It's called an "implicit data packet drop attack."

5. Detection Mechanism for EPDA and IPDA

This section describes EPDA and IPDA routing attacks The attacker's source may know which node is being attacked. Possibly a source node removed this node from the network. IPDA attacks are harder to spot than EPDA attacks due to protocol adherence and unpredictable packet loss. Data supplied to the attacker is discarded. This section discusses network configuration and detection method functionality.

5.1 Detection Algorithm for EPDA

i) In this first step of algorithm Attacker node (A) receives a RREQ message Initiated by source node (S).

ii) Node A starts an RREP message with a higher sequence number than that of the RREQ message that was just received.

iii) When an RREP message is received, node S builds a buffer and places the message there.

iv) Along with setting a timer (TIMER) of 10 milliseconds, Node S also placed the first RREP message in the buffer.

v) Until the TIMER expires, Node S will buffer any RREP messages it receives for a given RREQ message.

vi) In most cases, the RREP message received from node A will be ignored by node S.

vii) To lower the trust value to the node that sent the RREP message with the greatest sequence number, Node S will choose the RREP from its buffer that has a moderate sequence number.

viii) A node is regarded as an attacker node if its trust value falls below the required minimum.

ix) All network nodes know about the attacker node, hence none will send or receive control or data packets from it.

Figure 5 shows a situation that is used to teach people how to spot an EPDA attack. This section describes EPDA and IPDA routing attacks. The attacker's source may know which node is being attacked. Possibly a source node removed this node from the network. IPDA attacks are harder to spot than EPDA attacks due to protocol adherence and unpredictable packet loss. Data supplied to the attacker is discarded. This section discusses network configuration and detection method functionality.

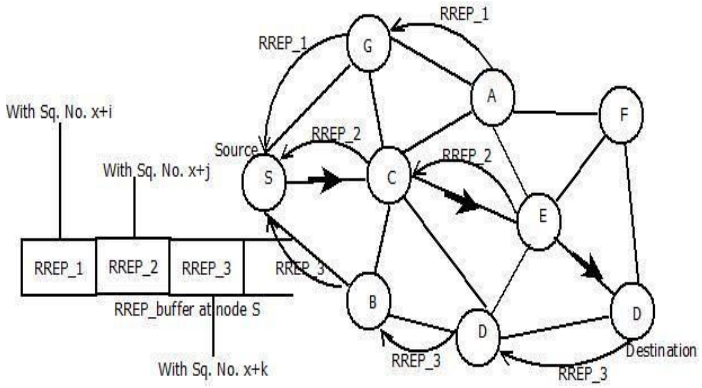


Fig 7 Detection mechanism for EPDA attack

This section describes EPDA and IPDA routing attacks. The attacker's source may know which node is being attacked. Possibly a source node removed this node from the network. IPDA attacks are harder to spot than EPDA attacks due to protocol adherence and unpredictable packet loss. Data supplied to the attacker is discarded. This section discusses network configuration and detection method functionality.

Detection Algorithm for IPDA

This section presents the detailed steps of the algorithm that can be used for the detection of IPDA attack. The steps of presented detection algorithm are as follow:

(i) In the beginning, each node in the network provides its neighbors a maximum trust value. When the trust level of a neighbor falls below the minimum, all communication between the two nodes will be disregarded.

(ii) As soon as the routing table is updated and data packets are sent out in response to an RREP message received by the source node, each data packet is given its own unique sequence number.

(iii) A node (N) that originates or forwards a data packet also sets a timer for T seconds and keeps an eye out for transmissions over the wireless channel.

(iv) As soon as the timer T ends, the node N will check to see if it's received the same data packet from its next-hop neighbor. Proximity listening on the wireless channel can be used for this purpose.

(v) If the timer for a particular packet has expired and Node N has not gotten a response, it will reduce the trust rating for its nexthop node. Other nodes on the network can then update or create a new trust record for the altered trust value of that node.

(vi) If Node N's next-hop neighbor regularly loses data packets, the trust value of Node N will continue to decrease

until it reaches the network's lowest acceptable trust value. At that time, all of the other nodes in the network will add Node N to their black list database.

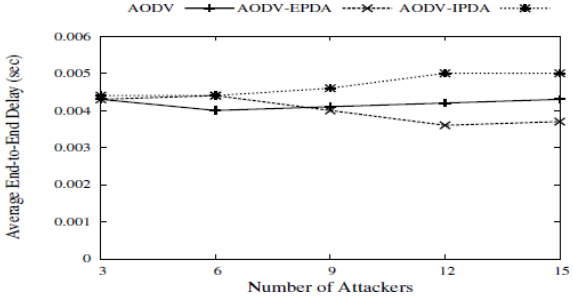


Fig 6 Average EED with increase in number of attackers

In other words, it's because the end-to-end latency depends on how long it takes to transmit a message. The distance between the starting point and the destination changes when looking for a route, just like the end-to-end latency. The source can choose a quicker, even more dangerous, route to the destination if an attacker is there, as this cuts down on overall time.

6. Simulation Result

AODV, AODV-EPDA, and AODV-IPDA are compared and evaluated in various network scenarios by modifying two parameters in the simulations:

• Increasing Number of Assailants: As time goes on, more and more sources will be added to keep up with demand. Network mobility was studied by modeling five different sources, The results are then multiplied by 10 Node mobility stays random between 0 and 10 m/s regardless of the number of sources.

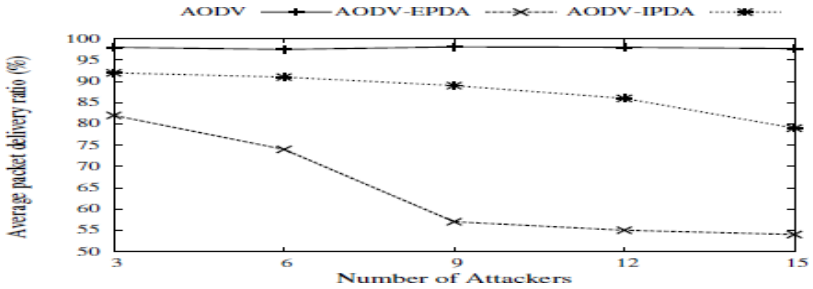
The impact of an increase in attackers on the network

To Avoid End-to-End Delay The number of attackers in the network rises as the end-to-end times for each comparative routing scheme do, as illustrated in Figure 6. The number of attackers on the network has little impact on the end-to-end transaction, as demonstrated in Figure 6. Average EED with an increase in the number of attackers is shown in table 1.

TABLE 1 Average EED with an increase in the number of attackers

Number ofAttackers	**AODV (insec)**	**AODV - EPDA (insec)**	**AODV - IPDA (insec)**
3	0.0043	0.0043	0.0044
6	0.004	0.0044	0.0044
9	0.0041	0.004	0.0046
12	0.0042	0.0036	0.005
15	0.0043	0.0037	0.005

Fig 7 Average PDR as the number of assailants rises



This graph shows how network packet delivery is impacted by attackers. This network consists of AODV, AODV-EPDA, and AODV-IPDA. As network attackers increase, packet delivery ratio drops.

TABLE 2 AVERAGE PDR WITH AN IMPROVEMENT IN ATTACKERS

No. ofAttackers	PDR inAODV(%)	PDR inAODV-EPDA(%)	PDR inAODV-IPDA(%)
3	98	82	92
6	97.5	74	91
9	98.1	57	89
12	98	55	86
15	97.7	54	79

As shown in Figure 7, the AODV-IPDA protocol is able to transport more packets than the AODV-EPDA protocol as depicted in table 2. The AODV-IPDA and AODV-EPDA routing algorithms are distinguished by the reduced probability of an attacker coming through an active route. Because of this, the differentiation is made, the third argument is to save money on transportation. Figure 8 depicts the rise in the number of AODV-EPDA and AODV-IPDA network attackers and the resulting increase in Routing Overhead. The network must conduct more work to keep up with the growing number of intruders (see Fig. 8) . Fig 8 Average overhead with increase in number of attackers. Figure 8 shows that the standard AODV is more expensive than the other two. Even if a route is real and destroyed, an attacker won't broadcast an error message. This reduces the likelihood of an attack destroying the route. There were fewer routes, An EPDA or IPDA can disable UDP-based MANETs (IPDA).

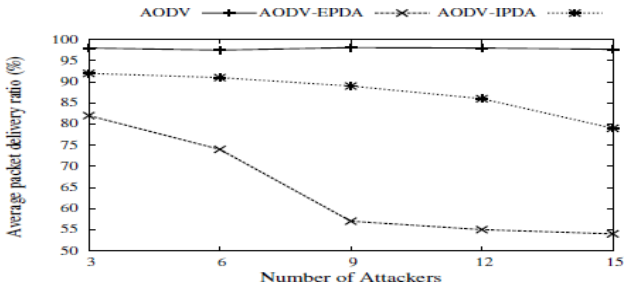


Fig 8 AVERAGE PDR WITH AN IMPROVEMENT IN ATTACKERS

As the number of attackers on the network increases, the chance that one is on an active route rises. Attackers can transmit extra data packets to target nodes as shown in table 3. When a network isn't under assault, discovery is more common.

TABLE 3 AVERAGE ROUTING OVERHEAD WITH INCREASE IN NUMBER OF ATTACKERS

Number ofAttackers(Node)	RoutingOverhead inAODV(%)	RoutingOverhead inAODV-EPDA(%)	RoutingOverhead inAODV-IPDA(%)
3	12	9	10
6	11.5	8	9.5
9	12.2	7.5	8.5
12	13	6	8
15	10.9	5	7

7. Conclusion

The work discussed in this study was created by fusing theoretical and simulation results. These packets will be discarded rather than forwarded by the attacker, increasing the number of packets that are lost. When more malicious users get access to a network, the overall packet delivery ratio worsens. As shown in Figure 7, the AODV-IPDA protocol is able to transport more packets than the AODV-EPDA protocol. The AODV-IPDA and AODV-EPDA routing algorithms are distinguished by the reduced probability of an attacker coming through an active route. Because of this, the differentiation is made. The third argument is to save money on transportation. Simulation findings show how attacks affect routing overhead, packet delivery rate, and end-to-end delay. Fewer attackers, but those that do deal the most damage. This chapter's simulation results show that the attacks are effective and affect data transfer. Using performance measures, the effects of network attacks are shown. The attack algorithms are precise

and powerful (such as End-to-End Delay, Packet Delivery Ratio, and Routing Overhead). This security method uses a central certification authority and key management scheme, which makes it easily extensible and less complex in computation, thus satisfying practically all security criteria. Nodes' energy needs are greatly reduced because very little computational overhead is produced. Built on top of the standard AODV routing technology, the newly proposed security system performs admirably. The proposed method is a good way to secure the AODV routing protocol because it uses less energy and works better against both hostile and unauthenticated nodes.

8. REFERENCES

[1] Perkin C.E.,Royer,E.M., "Ad-hocon demanddistancevector routing"in Proceedings of 2nd IEEE WorkshoponMobile Computer Systems and Applications, New Orleans,1999.

[2] VijayChhari, Rajesh Singh, and S.S. Dhakad, " Enhanced and more secure AODV routing protocol to avoid black hole attack in MANET", IJCSNT, 2014.

[3] Ellahadi M.Shasshuki,,Nan kang ,"EAACK-A secure intrusion Detection system for MANETs" IEEE transaction on Industrial electronics,Vol-60 N0-3 March 2013 Bhatia T, Verma AK (2013) Security issues in MANET: a survey on attacks and defense mechanisms. International Journal of Advance Research in Computer Science and Software Engineering 1382–1394.

[4] Gupta, S., Shahid, M., Goyal, A., Saxena, R. K., &Saluja, K. (2022, April). Black hole detection and prevention using digital signature and SEP in MANET. In 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22) (pp. 1-5). IEEE.

[5] Agrawal, J., & Kapoor, M. (2021). A comparative study on geographic-based routing algorithms for flying ad-hoc networks. Concurrency and Computation: Practice and Experience, 33(16), e6253.

[6] Rani, S., & Ahmed, S. H. (2015). Multi-hop routing in wireless sensor networks: an overview, taxonomy, and research challenges

[7] Rohokale, V.M.; Prasad, N.R.; Prasad, R. A Cooperative Internet of Things (IoT) for rural healthcare monitoring and control. In Proceedings of the 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Chennai, India, 28 February–3 March 2011; pp. 1–6.

[8] Ehsan, S.; Hamdaoui, B. A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Commun. Surv. Tutor. 2012, 14, 265–278. [Google Scholar] [CrossRef]

[9] ·Pawan&SusheelaHooda, 2021. "A New Approach for Power-Aware Routing for Mobile Adhoc Networks Using Cluster Head With Gateway Table," International Journal of Web-Based Learning and Teaching Technologies (IJWLTT), IGI Global, vol. 16(4), pages 47-59, July.

[10] M. Malnar, N. JevticAn improvement of AODV protocol for the overhead reduction in scalable dynamic wireless ad hoc networksWireless Netw (2022), pp. 1-13.

[11] Y. Trofimova, P. TvrdíkEnhancing reactive ad hoc routing protocols with trust

Future Internet, 14 (1) (2022), p. 28

[12] M. Kaur, D. Prashar, M. Rashid, Z. Khanam, S.S. Alshamrani, A.S. AlGhamdiAn optimized load balancing using firefly algorithm in flying ad-hoc networkElectronics, 11 (2) (2022), p. 252

[13] S. Li, X. Hu, T. Jiang, R. Zhang, L. Yang, H. HuHop count distribution for minimum hop-count routing in finite ad hoc networksIEEE Trans Wireless Commun (2022)

[14] Xu K, Hong X, Gerla M. An ad hoc network with mobile backbones. In: 2002 IEEE international conference on communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333), 2002, vol. 5: IEEE, pp. 3138–3143.

[15] Sharma, P., Nisha, Shukla, S. et al. An Era of Mobile Data Offloading Opportunities: A Comprehensive Survey. Mobile NetwAppl (2023). https://doi.org/10.1007/s11036-023-02116-8

[16] Lowe, D.G., 1999. Object recognition from local scaleinvariant features. Proceedings of the 7th IEEE International Conference on Computer Vision, Sept. 20-27, IEEE Xplore Press, Kerkyra, Greece, pp: 1150-1157. DOI: 10.1109/ICCV.1999.790410.

[17] Mohapatra, S. and P. Kanungo, 2012. Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator, Procedia Eng., 30: 69-76. DOI: 10.1016/j.proeng.2012.01.835.

[18] Duan, Y., C. Borgiattino, C. Casetti, C.F. Chiasserini and P. Giaccone et al., 2014. Wi-fi direct multigroup data dissemination for public safety. Proceedings of the World Telecommunications Congress, Jun. 1-3, IEEE Xplore Press, Berlin.

[19] Felice, M.D., L. Bedogni and L. Bononi, 2016. The emergency direct mobile App: Safety message dissemination over a multi-group network of smartphones using wi-fi direct. Proceesings of the 14th ACM International Symposium on Mobility Management and Wireless Access, Nov. 13-17, IEEE Xplore Press, Malta, pp: 99-106. DOI: 10.1145/2989250.2989257

[20] Sharma, N., Soni, M., Kumar, S., Kumar, R., Deb, N., &Shrivastava, A. Supervised Machine Learning Method for Ontology-based financial decisions in Stock Market: Ontology-based financial decisions in Stock Market. ACM Transactions on Asian and Low-Resource Language Information Processing.