Volume 65, Issue 3, 2021

Journal of Scientific Research

Institute of Science,
Banaras Hindu University, Varanasi, India.

Asymmetric Key Cryptography based Ad-hoc on Demand Distance Vector Protocol (AC-AODV)

Awadhesh Kumar*

Computer Science-MMV, Banaras Hindu University, Varanasi, India. bhuipsbhu@gmail.com*

Abstract: **Disaster is sudden, catastrophic events which origins are natural calamities and man-made, cause greater loss, damage and destruction of life and property. Since there are several geographical areas in the globe in which natural calamities such as flood, earthquake, hurricanes, landslides, cyclones, volcanic eruptions, tsunamis, storms etc. and man-made disaster likes rescue operation, terrorist and Naxalite attacks are more common. Hence it is too expensive to establish infrastructure based cellular network because it may not provide solution to the users in the areas in which such types of calamities mostly happens. Mobile ad-hoc network (MANET) is one of the best solution in affected areas as discussed above because it is infrastructure less network and setup anywhere and anytime. MANET have some issues like lack of centralize monitoring, open standards, narrow bandwidth, mobility, storage, and variation in link hence security is much more required than the wired network. Ad-hoc On-Demand Distance Vector (AODV) routing protocol reduces control packet overhead, adaptability with dynamic changing network, low setup delay, and less memory requirement but suffer from various attacks such as impersonation, byzantine, black whole and resource consumption attack. To address the security vulnerabilities and shortcomings of previous methods, we proposed an asymmetric key cryptography-based scheme for securing the AODV (Ad hoc On-Demand Distance Vector) routing protocol in this paper.**

Index Terms: **MANET's, Cryptography, AODV, Authentication, Route Exploration, and Route Management.**

I. INTRODUCTION

Cryptology is the way of securing message and analyzing the security breaches. Cryptography and cryptanalysis are the two main branches of cryptology that are used for hiding the data or message and analyzing the various attacks/breaches simultaneously(Press, n.d.). MANET is an infrastructure less network with limited resources hence designing routing strategy for MANET is a challenging task(Beraldi & Baldoni, 2002). For efficient and reliable routing with limited resources, an intelligent routing strategy is required and is being adaptable to the changing network parameters including network capacity, traffic density, and network partitioning to different kinds of applications and consumers can have different degrees of QoS. (Mchergui et al., 2017). In mobile ad-hoc networks, the routing protocol can be divided into three groups such as global/proactive, on-demand/reactive and hybrid protocols (Perkins et al.; 1999,Kumar & Tewari, 2016). Routes to all destinations (or portions of the network) are determined at startup and managed using a periodic route updating mechanism in proactive routing protocols(B.D. & Al-Turjman, 2020; Zhang et al., 2018). In reactive protocols, route search process is initiated by the originator node through route exploration mechanism as necessitates their presence, and hybrid routing protocols combine the basic features of proactive and reactive routing protocols into one(Ko & Vaidya, 2000; Perkins et al., 1999). Here we discuss reactive routing protocols because it reduces the control packet overhead, memory requirement and setup delay as compared to proactive routing protocols by just keeping details about active routes. Route exploration and route maintenance are the two main component of a reactive routing protocol(Kaur et al., 2013). When there is a need for route from origin node to target node, origin node initiate a path exploration by advertising a route request packet (RREQ) to the neighbourers of origin node in a network and neighbour nodes forward the route request packet (RREQ) to our neighbours and this process continues till the route request reach to the destination or all possible route permutation has been examined(Kaur et al., 2013). Once a route between source to destination is entrenched then there is a route maintenance

* Corresponding Author

DOI: 10.37398/JSR.2021.650315

mechanism to preserve the route till the route is discontinued or destination becomes not accessible by any path from source(Panda & Pattanayak, 2018). If the route request has travelled via bi-directional connections, route reply is sent back from destination to source using link reversal or by piggybacking the route in a route reply packet through flooding (Panda & Pattanayak, 2018). Therefore, it may possible that in worst case the route discovery overhead will be increased.

II. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) PROTOCOL

The functionalities of destination sequence distance vector and data source routing protocols are combined in this protocol. This protocol makes use of the data source routing protocol to discover and manage routes, as well as the DSDV principle for hop-by-hop routing, sequence number, and periodic beacons.(Al-Dhief et al., 2018). For establish and maintaining MANET, this protocol reduces the number of required broadcast because it forge routes when demanded and permit dynamic, multi-hope routing between participating mobile nodes(Kratzert & Krossing, 2018). AODV requires an only source and destination node as compared to data source routing which requires the complete information of route path between source and destination. The three types of AODV messages are Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs). (Kumar & Tewari, 2017b). The protocol does not keep track of which nodes are connected to which other nodes and determine a path only when it is absolutely necessary, and each node maintains a sequence number that is steadily growing each time the node notices a shift in the neighbourhood topology(Kumar & Tewari, 2017b). The AODV protocol is based on a broadcast exploration scheme and route management, and data is stored in a table in the format: <<destination address, next-hop address, destination sequence number, and life time>>.(Kumar & Tewari, 2016). Consider the following scenario: a sender node S explores a path by broadcasting information to every nodes of its neighbours, each node that accepts the information from S ahead the information to its immediate neighbours, and this process proceeds in a chain structure until the message reaches the final destination D, assuming D is reachable from sender $\boldsymbol{S}$ (Kumar & Tewari, 2017b). After establishing path, reverse route reply is send back by destination node D to source node S.

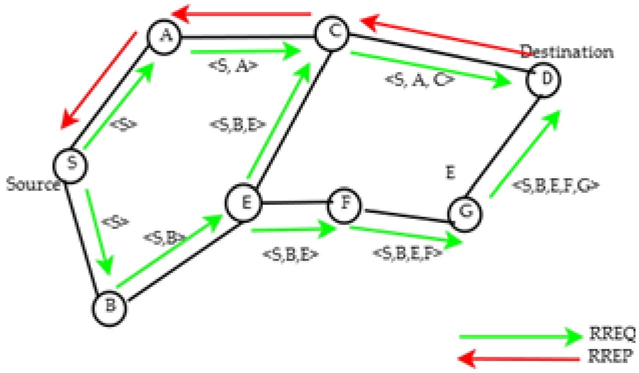

Fig. 1: Route Exploration in AODV protocol

The route will be maintained as long as it is operational, which is described as data packets travelling from the source to the destination along the path on a regular basis. (Perkins et al., 1999). The link will time out and be deleted from the intermediate node routing tables, once the origin ceases transmitting packets(Zapata, 2002). During the active route, if a connection is broken, the route error message (RERR) will be propagated through break upstream to source node about an unreachable destination and after receiving route error message, source node can start the route exploration process all over again if route desired. The downside of AODV is that the node can encounter substantial delays during route building, and connection failure can result in a new path exploration, which creates more delays and demands more bandwidth as the network grows in size. (Lee et al., 2003).

III. SECURITY FLAWS IN AODV:

Since the AODV protocol lacks a valid mechanism to avoid various security vulnerabilities, a compromised node 'M' may carry out a variety of attacks against AODV by violating the AODV rules.

- An impersonation attack occurs when a compromised node pretends to be a source node by falsifying a route request with its address as the discoverer address, and then pretends to be a destination node by falsifying a route reply with its address as the destination node address(Kavitha & Mukesh, 2018).
- A modified sequence number and hop count attack occurs when an origin node initiates and ahead a path request to explore a destination and a malicious node reduces the hop count field and increments the sequence number to fool other nodes into thinking this is the most recent route (Abdelshafy & King, 2013).
- Even if no connection is broken between source and intermediate nodes, a malicious node will send route error (RERR) information about the broken link to the origin node, causing the origin to restart the path exploration operation again. This type of attack is known as falsifying route error attack(Abdelshafy & King, 2013).
- Attackers capture packets in one network region, route them to another, and advertised them through entire network. This type of attack is known as wormhole attack(Jamali & Fotohi, 2016; Patel et al., 2015).
- A black-hole attack happens when a compromised node claims to have shortened route to any desired node in the network despite actually having no route to that nodes which results, all packets can travel through it, which results during data transmission, the black-hole node will forward or discard packets(Tamilselvan & Sankaranarayanan, 2008).
- A resource utilization attack occurs when a compromised node attempts to drain the intended ad-hoc wireless network's scarce usable resources, such as battery capacity, computing capability, and bandwidth from additional nodes in the network.(Abdel-Fattah et al., 2019).
- Byzantine attack is a form of attack in which any or a group of intermediate agreed nodes collaborates to carry out attacks such as building routing loops, forwarding packets on non-optimal routes, and selectively dropping packets, all of which cause routing services to be disrupted or degraded(Awerbuch et al., 2002).

IV. Asymmetric Cryptography based Ad-hoc on Demand Distance Vector Routing Protocol (AC-AODV)

Since AODV has many security vulnerabilities, as discussed above, cryptographic certificates are used with the Ad-hoc on Demand Distance Vector routing protocol to include security principles such as confidentiality, integrity, and non-repudiation. (Kumar & Tewari, 2017b), and cryptographic certificates of this kind are now being used in one-hop 802.11 networks. (Karlof & Wagner, 2003). The proposed routing protocol provides various security resources such as message integrity, authentication, and non-repudiation (Kumar & Tewari, 2017a) that offers a solution to the above security vulnerabilities. The objective of proposed protocol is as follows:

- The sender creates a digital signature using own private key and sends it along with a message to the recipient. The recipient verifies the digital signature using the sender's public key, ensuring that the signature was made by the sender alone and not by someone else. This procedure guarantees all messages are authenticated.
- Public key cryptography is used in the protocol for encrypting and decrypting the message and if any alteration of either the message or digital signature will cause the digital signature verification function to yield a value of false, indicating that the verification is failed. This shows the message integrity
- The Protocol uses digital signature for signing and verifying the message. Digital signature ensures the non-repudiation.
- The Proposed protocol includes certification process followed by route exploration and route management process that ensure end to end authentication.

The various notations used in proposed protocols during the communication among the nodes in MANET are listed in the table1.

Table I: Variables and their description used in proposed AC-AODV Routing Protocols

Variables	Description	Variables	Description
CertA	Certificate of node A	N_S	Nonce issued by node S
t	Time Stamp	IP_S	IP address of node S
e	Expiration time of certificate	SRV	Packet Identifier for the shortest route validation
K_{S+}	Node S's public key	REP	Reply Packet Identifier
K_{S-}	Node S's private key	RDP	Packet Identifier for Route Discovery
$\{d\}K_{S+}$	Encryption of data d using node S's public key	ERR	Identifier for Error Packets
$\{d\}K_{S-}$	The private key of node S digitally signs data d.	REQ	Identifier for Request Packets

A. Route exploration in proposed AC-AODV protocols:

In the AC-AODV protocol, route exploration is initiated by an origin node in such a way that broadcasting message is authenticated at each hop and when the message reaches to their target destination, it setup reverse route reply request information to origin in similar ways. The route discovery process in proposed AC- AODV consists of two stages. First stage is known as certification process in which before allowing a node into the ad-hoc network, the mobile ad-hoc network lets one of the nodes function as a trusted server, which issues a certificate to each node of the network. Any node A joining the MANET received the following certificate from the trusted server node T.

$$T \rightarrow\ A\colon Cert_A =\ [\ IP_A, K_{A+}, t, e]\ K_{T-}$$

The IP address of node A, the public key of A, the time stamp t indicates the certificate's development time, and e indicates the certificate's expiration time are all included in the certificate provided by trusted server T to node A and using its own private key, trusted server T concatenates and signs these components. Any node in the mobile ad-hoc network has a new certificate from trusted server T, and they must know the server public key (K_{T+}) . This guaranteed end to end authentication because when route exploration is initiated, the objective of the source node is to certify that the esteemed target destination has been reached. The origin nodes trust the target destination to take decisions to use Route Request (RREQ) and Reverse Route Request Reply (RRREP) as a return path(Kumar & Tewari, 2017b).

1) Route Request Exploration with Authentication:

The process of route request exploration in asymmetric key based secure AODV routing protocols are as follows:

1. For finding the route from source to destination, source node S initiates path discovery by broadcasting route request (RREQ) packets to its neighbours in the format shown below.
   $$S \rightarrow\ broadcast\colon [RREQ, IP_X,\ Cert_S,\ N_S, t]K_{S-}$$
   the route request message include the route request packet type identifier(RREQ), destination node IP address(IP_X), certificate of origin node $Cert_S$, the current time t, a nonce N_S , and message is signed with origin node private key K_{S-}. Nonce N_S is monotonically increasing each time when source node initiate a path exploration, other nodes receiving the RREQ packet stored the nonce they last saw with its corresponding timestamp.
2. When an intermediate node receives an RREQ, it keeps track of which neighbour sent it.
3. Intermediate node signed the packet content and rebroadcast it to each of its neighbours. This mechanism prevent spoofing attack. Consider node A is the neighbour of node S, then A receive the packet from source node S and rebroadcast it in the form:
   $$A \rightarrow Broadcast\colon \big[[RREQ, IP_X\,, Cert_S, N_S, t]K_{S-}\big]K_{A-}, Cert_A$$
   Any intermediates node does not rebroadcast the duplicate packet because they have already seen the tuple(N_S , IP_S).
4. If node B is a neighbour of node A, then upon receiving node A's broadcast, node B validates the packet signature with the given certificate. After deleting node $A's$ signature, node B rebroadcasts the RREQ to its neighbours, culminating in
   $$B \rightarrow Broadcast\colon \big[[RREQ, IP_X\,, Cert_S, N_S, t]K_{S-}\big]K_{B-}, Cert_B$$
   and similarly for other nodes
   $$C \rightarrow Broadcast\colon \big[[RREQ, IP_X\,, Cert_S, N_S, t]K_{S-}\big]K_{C-}, Cert_C$$
   $$D \rightarrow Broadcast\colon \big[[RREQ, IP_X\,, Cert_S, N_S, t]K_{S-}\big]K_{D-}, Cert_D$$
5. Upon receiving the first RREQ packet with correspondence nonce by target node X, the target node verify the signature and certificate upon receiving route request.
   $$X \rightarrow Receive\colon \big[[RREQ, IP_X\,, Cert_S, N_S, t]K_{S-}\big]$$

2) Exploration of Reverse Route Request Reply with Authentication:

When the message arrived at its target destination, it replies to the first route discovery process (RDP) that the destination receives from the source with a given nonce. In this process it is not guaranteed that the message received by source node from destination travels through shortest RDP. If any congestion or network delay rendezvous due to legitimately or maliciously manifested node then shortest route may be stopped from being the first to arrive at the destination and hence for reduction in the delay, non–shortest or non-congested path is preferred in such scenarios. In this process, the malicious node has no chance of redirecting the traffic because the message is signed on each hop. When destination node X received the route request from origin node, node X setup replies back by using the reverse route request reply (RRREP) path as in route discovery process and assume that node D is the first node on the path back to X and node X sends a Route Reply (RREP) to node D and this process continue using reverse route request reply till reverse route reply request reaches to source node S. In reverse route reply process, when primary path (shortest path in which RREQ reach to destination) fails to send route response from target destination to source then if another available alternate direction exists, route reply reaches the target destination to the source. In this way, avoid the problem of unicast route response and also provide multicast route response from target destination to source as source node initiate a RREQ that occurs in AODV protocol. This approach is advantageous when during the unicast route reply, some nodes leave from the network or power failure or other types of problems occurs with the node and it does not respond and generate a route error. In this situation approach reduces the control packet overhead. The reverse route request reply is sent from destination node to source node as follows:

$$X \rightarrow D: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]$$

$$D \rightarrow C: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]K_{D-}, Cert_D$$

$$C \rightarrow B: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]K_{C-}, Cert_C$$

$$B \rightarrow A: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]K_{B-}, Cert_B$$

$$A \rightarrow S: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]K_{A-}, Cert_A$$

$$S \rightarrow Recieve: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]$$

Suppose node A fails to receive the route reply from node B and in such situation if unicast route reply is used, then source node S receives a route error and reinitiate the route exploration procedure. In the proposed approach gives the solution of above situation and node B also rebroadcasts the reverse route reply to node E and node E rebroadcast the reverse route request reply to node F and node F rebroadcast reverse route request reply to source node S. As a result, source node S receives the route reply message from destination node X through the path. $X \rightarrow D \rightarrow C \rightarrow B \rightarrow E \rightarrow F \rightarrow S$.

$$B \rightarrow E: \left[[RREP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{B-}, Cert_B$$

$$E \rightarrow F: \left[[RREP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{E-}, Cert_E$$

$$F \rightarrow S: \left[[RREP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{F-}, Cert_F$$

$$S \rightarrow Recieve: \left[[RREP, IP_S, Cert_X, N_S, t]K_{X-}\right]$$

In the process discussed above, the nonce and signature of the previous hop are checked by each hop of the route when the source receives a response from the destination through the reverse route. As source node S receives a route reply from destination node X, it verifies the destination node's signature and nonce. Since only the destination can address the RREQ packet, and other routes with the path to the destination cannot respond on its behalf, this mechanism prevents attacks in which a malicious node interrupts routes by impersonation and repetition. Freedom from loops can be conveniently ensured since destination is the only node that can initiate an RREP.

3) Shortest Path Confirmation Stage:

Shortest path confirmation stage is performed after establishing the shortest path and in this phase, a certificate for the destination node is needed. Data transmission can be pipelined in this phase using the shortest path exploration operation that was used in the previous phase. Consider an example in which origin node S initiate shortest route exploration and transmit the message to neighbours in the format given below:

$$S \rightarrow Broadcast: SRV, IP_X, Cert_X\left[[IP_X, Cert_S, N_S, t]K_{S-}\right]K_{X+}$$

The shortest path validation (SPV) message start with SPV identifier then the IP address of the destination node IP_X and certificate $Cert_X$ of X. The signed message was concatenated by the source, which included the destination IP address, its own certificate, a nonce, and a time stamp. The output of this signed message is then encrypted using public key of destination node X, so that no other intermediate node will change it. Receiving this message, intermediate neighboured nodes rebroadcast it with the following cryptographic credentials:

$$B \rightarrow Broadcast: SRV, IP_X, Cert_X\left[\left[\left[[IP_X, Cert_S, N_S, t]K_{S-}\right]K_{X+}\right]K_{B-}, Cert_B\right]$$

In this process, nodes do not forward duplicate packets because it updates the entries in their routing table. In addition, these entries also serve the route to reply packets from the target destination to source of the opposite direction path. After verifying that all signatures are correct, the destination node X sends a recorded shortest path (RSP) packet to the source node ‘S' from its predecessor node, say ‘D.'

$$X \rightarrow D: [RSP, IP_S, Cert_X, N_S, Route]K_{X-}$$

$$D \rightarrow C: \left[[RSP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{D-}, Cert_D$$

$$C \rightarrow B: \left[[RSP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{C-}, Cert_C$$

$$B \rightarrow A: \left[[RSP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{B-}, Cert_B$$

$$\mathrm{A} \rightarrow S: \left[[RSP, IP_S, Cert_X, N_S, Route]K_{X-}\right]K_{A-}, Cert_A$$

In the route maintenance activity of AC-AODV protocol, the routes are active when the nodes keep track Otherwise, where no traffic occurs on an existing path, the route is deactivated in the routing table. Nodes produce an Error (ERR) message when data is received on an inactive route which is sent back to the source node. Nodes also send ERR messages to report broken connections in active routes as a result of node movement. Consider the following scenario: a node B emits the ERR message for its neighbour C on a path between source S and destination X as follows:

$$B \rightarrow C: [ERR, IP_S, IP_X, Cert_b\ N_b, t]K_{B-}$$

This message has been dispatched without making any changes in the way to the source. A nonce and a timestamp keep the ERR message fresh. The compromised node cannot produce an error message for the rest of the nodes since the error messages are signed. Since the error message is signed which shows the non-repudiation allows node to be identified as source node. This approach is beneficial because

- Malicious node requires valid certificate to increase the length of shortest path confirmation (SPC), which is not possible.
- The compromised node would not be able to shorted or alter the length of recorded path.

V. Security Analysis of AC-AODV

In this section, we examine how secure an asymmetric cryptographic-based ad hoc on-demand distance Vector routing protocol is against some of the previously discussed attacks.

- Unauthorized node participation in the network can be restricted because all the participated mobile nodes of Ad-hoc networks accept the packet only when packets signed with certificate issued by trusted server.
- This approach prevent the impersonation attack because only source nodes can sign with their private keys during route exploration and nodes cannot fraud with other nodes in route establishment. Only the destination node's certificate and signature are included in reply packets, meaning that only the destination will respond to route exploration.
- Modification Attack can be prevented by proposed asymmetric cryptography based AODV (AC-AODV) because it states that between source and destination, RDP and REP packets retain all of their fields. Since all control packet formats are signed by the initiating node, all modifications in transit will be automatically detected by intermediate nodes along the way and the altered packet will be discarded.
- In proposed AC-AODV protocol prevents replay attacks by using a nonce and a timestamp for routing signals.

VI. Simulation and Result Analysis

A. Simulation parameters and Environment

The performance matrices discussed below determine the success of proposed AC-AODV protocol over a simple AODV protocol.

Packet Delivery Ratio [PDR]: The packed delivery ratio is calculated by dividing the number of packets successfully delivered to the destination by the number of packets generated by the source. (Amirah et al., 2019).

$$PDR = \frac{Total\ packet\ received\ by\ the\ receiver}{Total\ Packet\ send\ by\ sender}$$

Delay: The interval between the origin node initiating the path request and the destination node receiving the first data packet is known as the path delay. It is determined by the nodes location and mobility(Al-Dhief et al., 2018).

$$Time\ Delay = \\ Time\ when\ first\ data\ packet\ arrives\ at\ destination\ - \\ Time\ when\ the\ RREQ\ message\ is\ broadcast\ by\ the\ origin\ node$$

Control Packet overhead[CPO]: The ratio of number of packets sent multiply by size of packets to packet received by destination and multiply by size of received packet(Science, 2019).

$$CPO = \frac{routing\ packet\ sent * size\ of\ date\ packet}{Received\ data\ packet * Size\ of\ received\ data\ packet}$$

Routing Load (bytes): It's the ratio of delivered overhead bytes to data bytes. In comparisons to AODV protocol, the proposed authenticated AODV contained certificates and signatures, protocols have a higher control overhead due to certificates hence get higher control overhead packets(Maan & Mazhar, 2011).

Average Path Length: The average number of hops a data packet must travel to reach its final destination. (Pal et al., 2013).

Average Route Acquisition Latency: The time it takes for a source node to start path discovery to a destination and for the source to receive the first route reaction from the destination. If the path exploration has to be restarted due to a timeout, the first transmitting time will be used to compute latency(Doshi & Kilambi, 2003).

Average End-to-End Delay of Data Packets: This type of delay encountered on the way to the destination at a series of intermediate nodes(Kumar & Tewari, 2016). This involves delays caused by transmitting, dissemination, sorting, queuing, and path acquisition, and among other things.

Simulation Environment

In this section, discuss about simulation environment. For simulating results, use simulator OMNeT++ which is a component-based, extensible C++ simulation library framework. In this simulation environment, we use INET framework which is an open source model library. The simulation is set up in various playground sizes, including 700m X 700m and 1000m X 1000m, with varying numbers of handheld nodes (Kumar & Tewari, 2017b). The parameters listed in table 2 were used to set up the OMNeT++ Simulation Environment.

Table 2: Simulation setup Environment(Kumar & Tewari, 2017b)

Dimensions of the Playground	700x700, 1000m X 1000m
Varies no. of nodes	10-50
Max. Channel Power	2.0 mW
Radio Tx. Power	2.0 mW
Radio Bitrate	54 Mbps
Broadcast Delay	0 to 0.008s
Simulation Time	600s
Start Time	0 s
Message Length	512B
Message Frequency	0.2s
Routing Protocol	AODV, AC-AODV
model	Random way point mobility model
Key Size	512 bit
Signature Size	128 bit

B. Result Analysis of AC-AODV Protocol without malicious node:

To evaluate the performance of asymmetric key cryptography based AODV protocol (AC-AODV) over simple AODV protocol, we study and analysed the results given below:

We can see from fig. 2 that the packet delivery ratio obtained using proposed AC-AODV routing protocol is approximately above 95% in all scenarios and is almost identical to the packet delivery ratio obtained using AODV when no malicious node presents. This shows that the AC-AODV routing protocol is extremely efficient at finding and sustaining routes, even though node mobility exists.

Fig. 3 shows routing load measurements over varying nodes speed and observed that in AC-AODV routing protocol, byte routing load is much larger, reaching 100% for 50 nodes moving at 10 m/s, as opposed to 46% for 50 nodes moving at 10 m/s using AODV protocols.. This significantly higher load (in bytes) is obtained due to the security of proposed protocols.

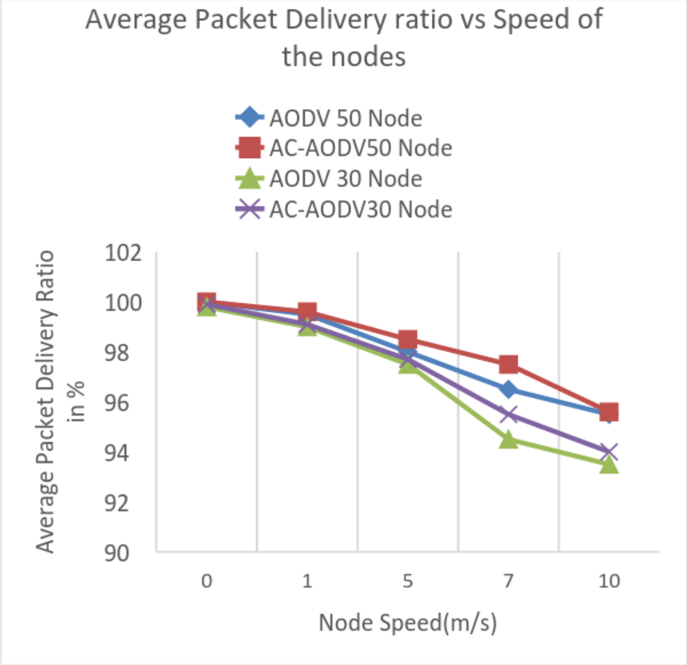

Fig.2: Average packet delivery ratio with varying node speeds

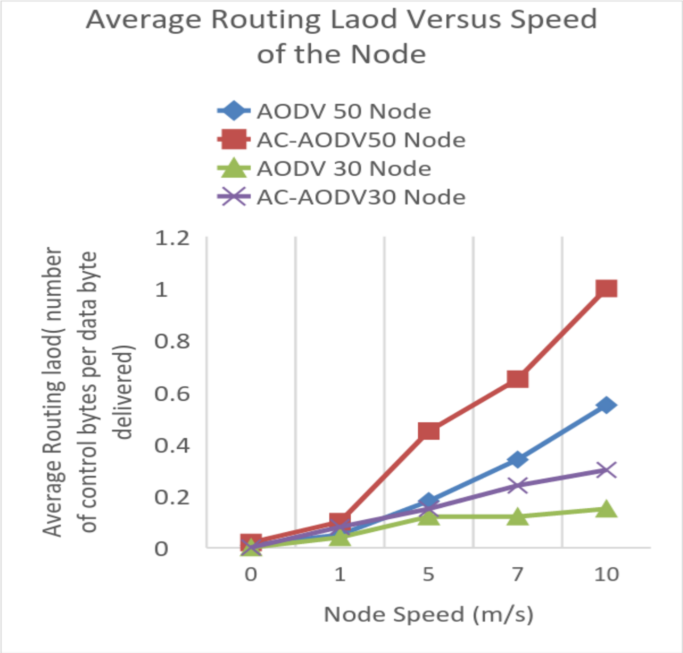

Fig. 3: Routing Load Average (# of control bytes delivered per data byte) with varying speed nodes

Fig. 4, shows that average data packet latencies with varying nodes and speeds for both protocols and we observed that, the two protocols in terms of data packet latency are again almost identical. Despite the fact that the total number of data packets sent is a minor proportion of the total number of path discoveries made, (as seen in the graph), so the proposed authenticated AODV routing protocols have higher route acquisition latency. As a consequence, route acquisition latency has negligible effect on average data packet end-to-end delay.

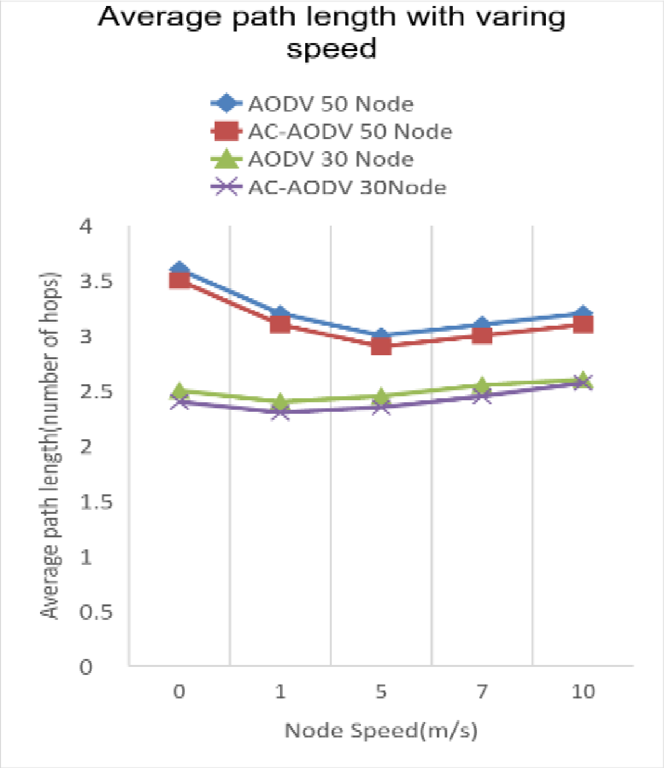

Fig.4: Average Data packet latency with varying nodes

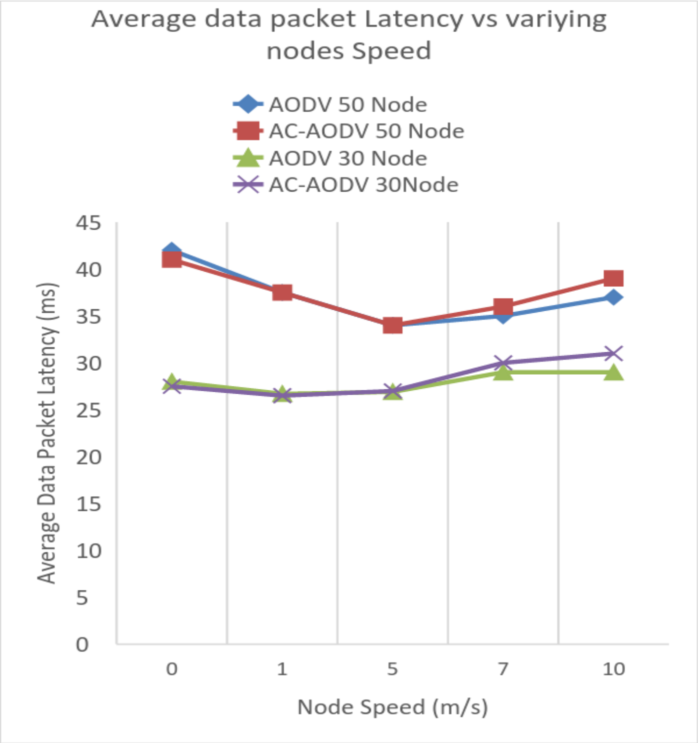

Fig.5: Average Path Latency with varying nodes

Fig. 5 depicts the average path length as a function of the number of nodes and speeds and observed that in the proposed Authenticate AODV and AODV protocols have almost equal average path length graphs. This shows that even though the proposed asymmetric cryptography based

AODV does not explicitly find the minimized path but the quickest route to destination search packet usually travels with the minimized path. This demonstrates that propose authenticated AODV is more successful than AODV for finding the shortest path. However in the network with significantly higher traffic load and even unicast route reply is fails, the suggested protocols often block the shortest path from being discovered. Fig. 6 depicts the average route acquisition latency in a network with different node frequencies. It was discovered that the proposed protocol's average route acquisition latency is roughly twice that of AODV. This is because in comparisons to AODV protocol, at each hop control packets in an asymmetric cryptography based secure AODV routing protocol verifies the previous node's digital signature before replacing it with its own digital signature. In a proposed protocol route acquisition latency is increased because of delay at each hop caused by signature generation and verification. During the experiment, we also observe that when the number of hops in the network is less, AODV route acquisition latency is significantly greater than the latency of proposed protocols.

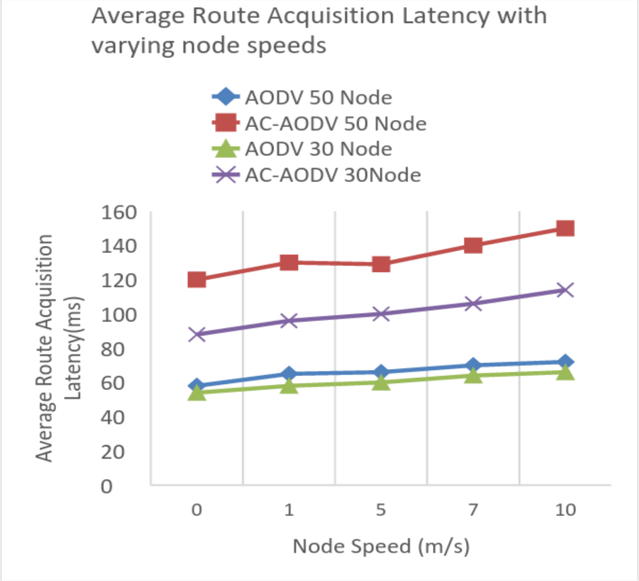

Fig.6: Average Route Acquisition Latency with varying node speeds

C. Effect of Malicious Node Behaviors in Proposed Asymmetric Cryptography based AODV (AC-AODV) Routing Protocol:

The impact of malicious node behaviour is evaluated for both proposed AC-AODV and AODV protocols using the aforementioned simulation scenario, which includes 50 nodes in a playground network of area 1000m X 1000m. The behaviour of the AODV protocol is influenced when multiple malicious nodes are present in the playground region during the simulation of the AODV protocol. The behaviour of Asymmetric cryptography based AODV and simple AODV protocol are tested when during the simulation, malicious nodes were present in proportions of 10%, 20%, and 30% and chosen at random. To measure the result we used metrics including Average Path Length and Percentage of data packets received that were intercepted by compromised nodes to assess the outcome. Figures 7 and 8 drawn above show the effects.

Fig.-7, shows the average path length when various malicious nodes present with varying speed of the nodes. In the presence of compromised nodes, the total path length for AODV increases by about 10%, according to the statistic shown in figure.

Fig. 8 depicts the percentage of data packets received that travel through malicious nodes as a function of node speed. It can be seen that when using AODV, a much higher percentage of data packets pass through malicious nodes than using proposed Authenticated AC-AODV routing protocols. After analyzing the results we found that when 10% of malicious nodes with no versatility is present, very less packet passes through malicious node using proposed protocols as compared to simple AODV protocol in which just double packet passes through malicious nodes.

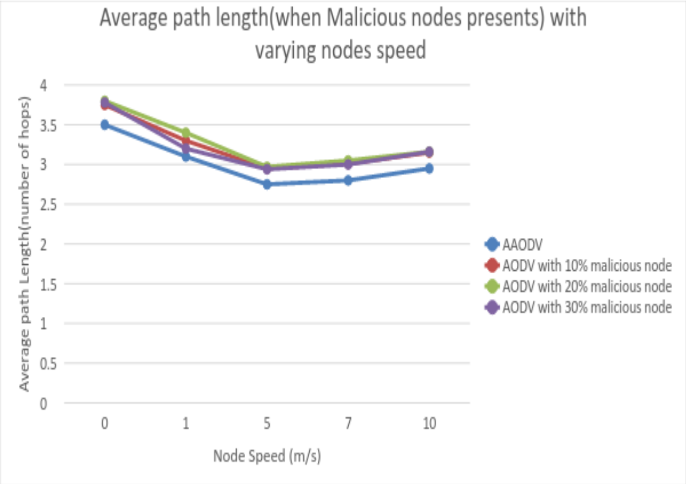

Fig.7: Average path length (when malicious nodes presents) with varying nodes speed

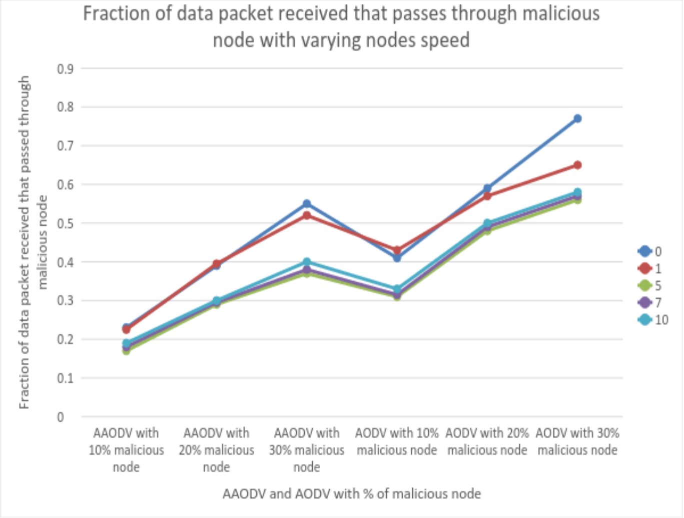

Fig.8: With different node speeds, the percentage of data packets obtained that travel through malicious nodes.

CONCLUSIONS

One of the most difficult problems in MANET is safe routing. In order to improve efficiency, we use asymmetric key cryptography based AODV routing which uses the principle of public key cryptography to provide security requirements such as authentication, integrity, and non-repudiation when establishing routes and transmitting data between MANET nodes. We have analyzed the performance of proposed asymmetric key based AODV protocol and compared it with the simple AODV protocols and found that average control packet delivery ratio, path length, and data packet latency is approximately same in both of the proposed and normal AODV routing protocol while average routing load to deliver bytes and packet are much higher in the proposed protocol than simple AODV protocol with varying speed of the nodes when there are no compromised nodes in the MANET network scenario. It is also found that when the malicious nodes percentage increases then proposed asymmetric key AODV protocol reduces the path length and very less fraction of packet are received from malicious node than simple AODV protocol.

REFERENCES

Abdel-Fattah, F., Farhan, K. A., Al-Tarawneh, F. H., & Altamimi, F. (2019). Security challenges and attacks in dynamic mobile ad hoc networks MANETs. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings*, *April*, 28–33. https://doi.org/10.1109/JEEIT.2019.8717449

Abdelshafy, M. A., & King, P. J. B. (2013). Analysis of security attacks on AODV routing. *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*, 290–295. https://doi.org/10.1109/ICITST.2013.6750209

Al-Dhief, F. T., Sabri, N., Salim, M. S., Fouad, S., & Aljunid, S. A. (2018). MANET Routing Protocols Evaluation: AODV, DSR and DSDV Perspective. *MATEC Web of Conferences*, *150*, 1–6. https://doi.org/10.1051/matecconf/201815006024

Amirah, N., Saudi, M., Arshad, M. A., Buja, A. G., Firdaus, A., Fadzil, A., & Saidi, R. (2019). *Mobile Ad-Hoc Network (MANET) Routing Protocols : A Performance Chapter 7 Mobile Ad-Hoc Network (MANET) Routing Protocols : A Performance Assessment Throughput Packet delivery ratio* (Issue January). Springer Singapore. https://doi.org/10.1007/978-981-13-7279-7

Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures. *Proceedings of the Workshop on Wireless Security*, 21–30. https://doi.org/10.1145/570681.570684

B.D., D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks*, *97*. https://doi.org/10.1016/j.adhoc.2019.102022

Beraldi, R., & Baldoni, R. (2002). *Unicast Routing Techniques for Mobile Ad Hoc Networks*. *Cnds*, 1–13. https://doi.org/10.1201/9781420040401.ch7

Doshi, J., & Kilambi, P. (2003). SAFAR : An Adaptive Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks. *ADHOC-NOW 2003, LNCS 2865*, 12–13.

Jamali, S., & Fotohi, R. (2016). Defending against Wormhole Attack in MANET Using an Artificial Immune System. *New Review of Information Networking*, *21*(2), 79–100. https://doi.org/10.1080/13614576.2016.1247741

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks : attacks and countermeasures. *Ad Hoc Networks, 1*, 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

Kaur, H., Sahni, V., & Bala, M. (2013). A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review. *International Journal of Computer Science and Information Technologies*, *4*(3), 498–500.

Kavitha, P. R., & Mukesh, R. (2018). Detection of Impersonation Attack in MANET Using Polynomial Reduction Algorithm. *International Journal of Network Security*, *20*(2), 381–389. https://doi.org/10.6633/IJNS.201803.20(2).19

Ko, Y., & Vaidya, N. H. (2000). Location-Aided Routing in mobile adhoc networks.pdf. *Wireless Networks*, *6*, 307–321.

Kratzert, D., & Krossing, I. (2018). Recent improvements in DSR. *Journal of Applied Crystallography*, *51*(May), 928–934. https://doi.org/10.1107/S1600576718004508

Kumar, A., & Tewari, R. R. (2016). Extended AODV Routing Protocol for Performance Improvement of MANET ' s. *International Conference on Advances in Computing, Control and Communication Technology*, *68*(2016), 59–68.

Kumar, A., & Tewari, R. R. (2017a). Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication. *International Journal of Computational Intelligence Research*, *13*(7), 1679–1698.

Kumar, A., & Tewari, R. R. (2017b). Symmetric Key Cryptography based Secure AODV Routing in Mobile Adhoc Networks. *Advances in Wireless and Mobile Communications*, *10*(5), 969–984.

Lee, S. J., Belding-Royer, E. M., & Perkins, C. E. (2003). Scalability study of the ad hoc on-demand distance vector routing protocol. *International Journal of Network Management*, *13*(2), 97–114. https://doi.org/10.1002/nem.463

Maan, F., & Mazhar, N. (2011). MANET Routing Protocols vs Mobility Models : A Performance Evaluation. *ICUFN 2011*, 179–184.

Mchergui, A., Moulahi, T., Alaya, B., & Nasri, S. (2017). A survey and comparative study of QoS aware broadcasting techniques in VANET. *Telecommunication Systems*, *66*(2), 253–281. https://doi.org/10.1007/s11235-017-0280-9

Pal, A., Prakash, J., & Dutta, P. (2013). The Path Length Prediction of MANET using Moving Average model. *Procedia Technology*, *10*, 882–889. https://doi.org/10.1016/j.protcy.2013.12.434

Panda, N., & Pattanayak, B. K. (2018). Analysis of blackhole attack in AODV and DSR. *International Journal of Electrical and Computer Engineering*, *8*(5), 3093–3102. https://doi.org/10.11591/ijece.v8i5.pp.3093-3102

Patel, A., Patel, N., & Patel, R. (2015). Defending against wormhole attack in MANET. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, *October*, 674–678. https://doi.org/10.1109/CSNT.2015.253

Perkins, C. E., Park, M., & Royer, E. M. (1999). Mobile Computing Systems and Applications (WMCSA '99). *Mobile Computing Systems and Applications (WMCSA '99)Ad-Hoc On-Demand Distance Vector Routing*, 90–100.

Press, A. (n.d.). *Real Life Cryptology Ciphers and Secrets in Early Modern Hungary*. https://library.oapen.org/bitstream/handle/20.500.12657/28452/1001507.pdf?sequence=1

Science, C. (2019). PERFORMANCE EVALUATION OF ROUTING ALGORITHM FOR MANET BASED ON THE MACHINE LEARNING TECHNIQUES. *Journal of Trends in Computer Science and Smart Technology (TCSST)*, *01*(01), 24–35.

Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. *Journal of Networks*, *3*(5), 13–20. https://doi.org/10.4304/jnw.3.5.13-20

Zapata, M. G. (2002). Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), 106–107. https://doi.org/10.1145/581291.581312

Zhang, D. gan, Zhang, T., Dong, Y., Liu, X. huan, Cui, Y. ya, & Zhao, D. xin. (2018). Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning. *Journal of Network and Computer Applications*, *122*(February), 37–49. https://doi.org/10.1016/j.jnca.2018.07.018

***