International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Secure and Efficient Data Transfer in AODV Routing Protocol Using RSA Encryption

Chatheka Ngazi Mangazi[1], Dr. Glorindal Selvam[2]

Master of Computer Science, DMI - St. Eugene university, Zambia
cmangazi[at]gmail.com

DMI - St. Eugene university, Zambia
gloryg. j[at]yahoo.com

Abstract: ***Mobile Ad - Hoc Networks (MANETs) are recognised as a key emerging technology for use whenever cellular communications are either infeasible, inefficient, or cost - ineffective. MANETS are composed of nodes that are arranged in a self – organizing manner, without a central device like a switch or router. The nodes communicate with each other over wireless links and cooperate in a distributed fashion. Smart phones are the most ideal network nodes in many of the scenarios where traditional networks are not available. But it is not as easy and straightforward to build a secure network with them. In this paper, we extensively use existing possibilities to build a secure MANET. The designed MANET has been built on an NS3 simulator, with the base protocol being Ad - hoc On - demand Distance Vector (AODV) and message encryption done by using RSA Algorithm. Therefore, we discuss our implementation of the Secure AODV protocol extension using RSA encryption.***

Keywords: MANET, AODV, Attack, RSA, and Encryption

1. Introduction

Whenever we talk of network communication in general, we often think about the sending and receiving device, or nodes, and some couple of intermediary or central devices like Switches, Access Points and Routers. These intermediary or central devices are there to route traffic from one network to another, link one device to another, regenerate, filter and forward the data signals and indeed change the signal from one form e. g., wired to another e. g. wireless. Traditional networks cannot function without one of these intermediary devices. Networks can either be wired or wireless, depending on the technology employed.

Devices in a MANET utilise wireless links only. This entails that they operate under the IEEE 802.11 standard framework. The IEEE 802.11 standard supports two distinct operation modes. These are Infrastructure Basic Service Set and Independent Basic Service Set. Independent Basic Service Set (IBSS) is also known as ad hoc mode and does not require any access points to be configured for its operation. IBSS however do not offer multi - hop capabilities, on their own. This is as such due to the fact that there must be path discovery, path selection and routing for multi - hop connectivity. These features are not available when Independent Basic Service Set is deployed on its own.

MANETs therefore, are an improvement of the Independent Basic Service Set as they do have mobile multi - hop connectivity and do not require any intermediary or central device for them to function. Being a self - configuring network of mobile devices connected by wireless links and with no central device like an Access Point or Switch, the nodes or devices in a MANET can send data to one another on their own. They also route traffic from one mobile device to another. This entails all devices have the capability to do path discovery and path selection in the network. This feature is unique in the sense that in traditional networks, path discovery, path selection and routing traffic are done by other specialised devices other than the nodes themselves. Nodes in a MANET are free to join or leave the network, or indeed to move haphazardly and organize themselves arbitrarily. The nodes density depends on the application of the MANET.

A MANET changes dynamically as mobile nodes join or leaves the network. The mobile devices in a MANET, or nodes act as a router, to receive and route messages from one node to another and vice versa. This feature of MANET entails that they extend the limited wireless transmission range of each participating node by employing multi - hop packet forwarding, and thus they are ideally suited for scenarios in which pre - deployed infrastructure support is not available, for example in times of natural disasters. However, the same capability of ease of configuration and nodes joining the MANET means security is a challenge.

Routing in a MANET is achieved by utilizing protocols. The protocols are mainly categorised as either Proactive, Reactive or Hybrid. Proactive routing protocols are table driven. In these protocols, each node maintains a separate routing table which has the information on the routes to all nodes in the network. This information is updated periodically. Reactive protocols are also known as on – demand protocols. This only query route information or discover new routing information when there is a need to send data to a particular node. Hybrid protocols on the other hand are the best of both worlds. They combine the advantages of both Proactive and Reactive routing protocols. They are adaptive to the zone and position of the source node and destination node.

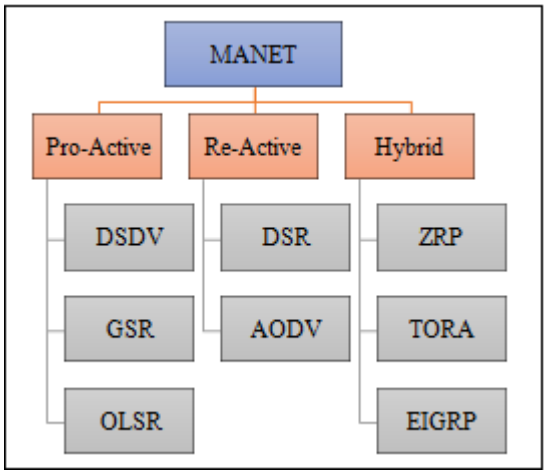

Figure 1: MANET Routing Protocols

Some of the prominent protocols, as depicted above, are Destination Sequenced Distance Vector Routing Protocol (DSDV), Global State Routing (GSR), Optimized Link State Routing Protocol (OLSR), Dynamic Source Routing protocol (DSR), Zone Routing Protocol (ZRP), Temporally Ordered Routing Algorithm (TORA) and Ad - Hoc On - Demand Vector Routing protocol (AODV).

AODV is a reactive routing protocol and an extension of DSR. It is reactive in the sense that path discovery is done only when there is a need to send data to a particular destination node and stores the path in the routing table. This is an On Demand approach to route discovery. It uses destination sequence numbers to identify the most recent path to a destination. DSR stores paths to destinations in the data packet's header itself. All the above protocols, on their own, do not offer security to the messages transmitted, thereby, are prone to numerous kinds of attack.

2. Challenges of AODV

MANET routing protocols have many vulnerabilities that may be exploited by malicious actors to disrupt the normal routing behaviour and the AODV protocol is not an exception to this. The operation of AODV protocol is that every mobile node has and continuously updates a routing table that stores the next - hop node information for a route to a destination node. When a source node (S) wishes to send a packet to a destination node (D), it uses the information in its table to route the traffic if such a route is available. Otherwise, node S initiates a route discovery procedure by broadcasting a Route Request (RREQ) message to all its neighbours. On receiving an RREQ message, the intermediate nodes firstly update the information in their own routing tables for a reverse route to the source node. All the intermediate nodes that have received the RREQ message but do not have a route to D, will further broadcast the RREQ packet to all neighbours. Intermediate nodes will then increment the hop - count before forwarding the RREQ. A Route Reply (RREP) message will thus be sent back to Sonce the RREQ reaches D. RREP may also be sent by an intermediate node that has a current route to D.

AODV routing protocol assumes that all nodes that have joined MANET are legal, and ideal and therefore will cooperate. However, this may not always be true. Malicious actors may take advantage of the route discovery process and compromise the network. This makes the protocol to be susceptible to numerous kinds of attacks, of which some are listed below.

2.1 Blackhole Attack

A black hole attack occurs when a malicious node sendsa Route Reply Packet (RREP) to publicize itself for having the shortest route to the destination node when in fact, it does not have any route to the destination. In this attack, the malicious node (M) constantly has the convenience of replying to the route requests for the desired destination node (D). The sending node (A) then will get this fake RREP and add the M as the next hop in its routing table. Now A will be sending packets to D through M. M will then be dropping these packets or indeed be sending them to another malicious node thereby creating a black hole in the network.

2.2 Gray hole Attack

Gray Hole Attack is an improved version of black hole attack. In this attack, the malicious node (M) may constantly or randomly drop packets and therefore reduce the efficiency of the MANET. Firstly, a malicious node manipulates the AODV protocol by broadcasting itself as having a fresh and valid route to a legitimate destination node. The intention, however, is to intercept packets, even though the route is bogus. Once this is achieved, the malicious node drops a certain percentage of the intercepted packets.

This kind of attack is more complicated and is therefore difficult to detect. This is so because of the fact that, received data packets are not dropped entirely, by the malicious node as in a black hole attack. A Gray - hole attack may exhibit its malicious behaviour in multiple fashions. It may drop packets coming from or transmitted to a certain specific node in the MANET while forwarding all the packets to other nodes without any malicious intent.

Furthermore, in a modified Gray - hole attack, a node may behave maliciously for a specified time frame by dropping packets and then switch to normal behaviour, by forwarding all traffic later. A Gray - hole may also exhibit actions which is a combination of the above two, thereby making its exposure even more complicated.

2.3 Flooding attack

A flooding attack is one of the DoS attacks that aim to exhaust the network resources by flooding the network with a lot of fake packets and messages. This kind of attack is achieved by a malicious node taking advantage of the route discovery process of the AODV routing protocol. The malicious node's intention is to flood the network with numerous RREQs to non - existent destinations in the network which in turn, takes a lot of the network resources. Since the requested destination does not exist in the network, a corresponding RREP packet cannot be generated by any node and therefore, all the nodes keep on flooding the RREQ packet.

When this large number of fake RREQ packets are broadcast into the network, new routes can no longer be added, as resources are channelled towards these fake RREPs and the network is unable to transmit data packets. Thus, it leads to congestion in the network and overflow of the route table in the intermediate nodes. The nodes cannot receive new RREQ packets, resulting in a DoS attack. The Flooding attack, therefore, has serious effects on MANET, as a result of the limited computational and power resources of nodes that are exploited.

3. Encryption Mechanism

Public key cryptography can be used to provide confidentiality and integrity of the routing information exchanged between nodes in the network. In this paper, we propose the use of the RSA Algorithm to implement Secure AODV protocol to prevent Black Hole, Gray Hole and Flooding attacks. RSA is a public - key cryptography algorithm that can be used to provide secure communication in a network. In this context, RSA is being used to provide secure communication between nodes in an AODV network. Our implementation of AODV with RSA encryption is depicted in the flowchart below:

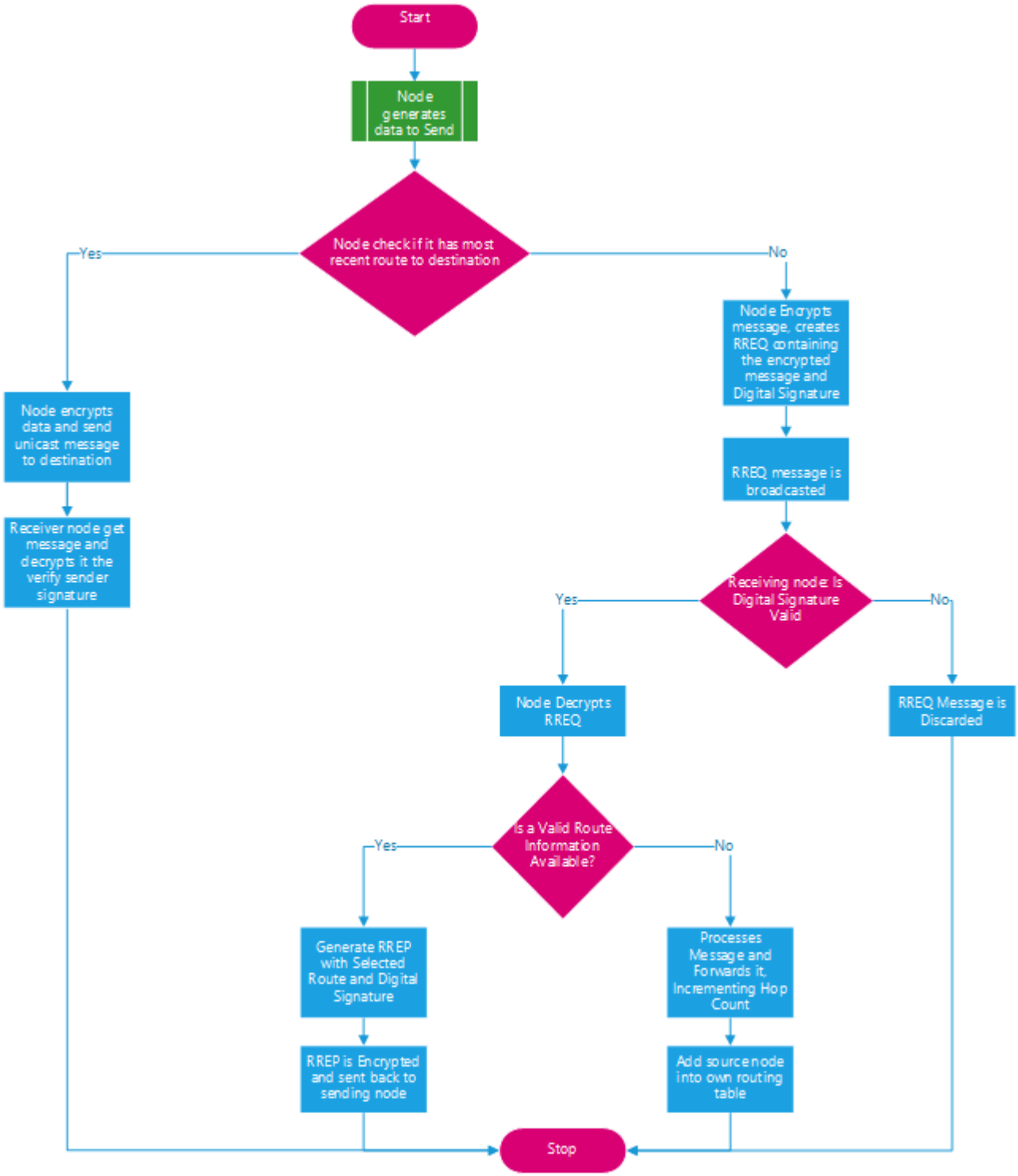

Figure 2: Flowchart for AODV with RSA encryption

The above flow is implemented in the following steps.

3.1. Key Generation:

a) This is the first step in the encryption process. Each node in the MANET generates a public and private key pair using the RSA algorithm. The key generation process involves the following steps:
- Select two large prime numbers p and q.
- Calculate n = $p * q$.
- Calculate the totient of n, phi (n) = (p - 1) * (q - 1).
- Choose an integer e, such that 1 <e< phi (n) and gcd (e, phi (n)) = 1.
- e is the public key exponent.
- Calculate d, the modular multiplicative inverse of e modulo phi (n). d is the private key exponent.
- The public key is (e, n) and the private key is (d, n).

3.2. Secure Routing Table

a) Each node maintains a secure routing table that contains information about the secure paths to other nodes in the network.
b) The routing table is encrypted using the node's private key to ensure that only the node itself can read the table.
c) To encrypt the routing table, each entry is encrypted using the node's private key.

3.3. Route Request (RREQ)

a) When a node wants to send a message to another node in the network, it first encrypts the message using the recipient node's public key.
b) The sender then creates a routing request message that contains the encrypted message and the sender's digital signature.
c) The digital signature is created by encrypting a hash of the routing request message using the sender's private key.
d) The routing request message is broadcasted to all the nodes in the network.

3.4. Route Response Reply (RREP):

a) When a node receives a routing request message, it first verifies the signature using the sender's public key.
b) If the signature is valid, the node decrypts the routing request using its own private key and selects the best route to the destination node based on the information in the table.
c) The node then creates a routing response message that contains the selected route and the node's digital signature.
d) The digital signature is created by encrypting a hash of the routing response message using the node's private key.
e) The routing response message is encrypted using the recipient node's public key and sent back to the sender.

3.5. Decryption

a) When a node receives a routing response message, it first decrypts the message using its own private key.
b) The node then verifies the signature using the sender's public key.
c) If the signature is valid, the node extracts the selected route from the routing response message and uses it to send the original message to the destination node.

3.6. Route Request Forward

a) When an intermediate node receives a Route Request (RREQ) message but does not have a path to the destination, it will process the message and forward it to its neighbouring nodes.
b) The intermediate node will read the unencrypted part of the RREQ message, which contains information about the source and destination nodes, as well as other parameters.
c) It will then increment the hop count in the message before forwarding it.
d) Intermediate node will then add the source node path into its own table.

4. Simulation Tests and Results

The above implementation was run in NS3 simulator. NS3 is a robust network simulation software and supports mobility, WIFI models and MANET routing protocols. It also supports an animation tool NetAnim, which visualises the simulation.50 nodes are set up and measured across three metrics of end - to - end delay, packet delivery ratio and throughput. The nodes send data at a rate of 2 Mbps for a duration of 300 seconds and the nodes move randomly. The size of each message sent is 512 bytes. The nodes use WiFi 802.11b in ad hoc mode and transmit at random speeds.

Table 1: Simulation results

Metric	Result
Throughput (Mbps)	1.7
PDR (%)	94
End to End delay (ms)	70

5. Conclusion

In this paper, we design a security extension to the AODV protocol to provide reliable and efficient data transmission and fend off attacks. Here we employ the RSA encryption Algorithm, which is using Asymmetric cryptographic technique. The implementation of the encryption mechanism has enhanced the security of the protocol and the MANET itself. The encryption and decryption of data packets and exchange of keys is used to enhance security in AODV protocol. Thus, we have designed an efficient and secure MANET.

References

[1] Prashant Kumar Maurya et al, An Overview of AODV Routing Protocol.2012
[2] L Raja and Capt. Dr S Santhosh Baboo, An Overview of MANET: Applications, Attacks and Challenges.2014
[3] Nitesh Funde and P R Pardhi, Analysis of Possible Attack on AODV Protocol in MANET.2014

[4] N Bhaskar and N. Sakthivel, MCA. Implementation of MANET: Application, Attack and Challenges
[5] T. Alam and M. Aljohani, "An approach to secure communication in mobile ad - hoc networks of Android devices, " 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, Japan, 2015, pp.371 - 375, doi: 10.1109/ICIIBMS.2015.7439466.
[6] Jaydip Sen et al, A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks.2021
[7] Abdelshafy, M. and King, P. J. B, Analysis of security attacks onAODV routing.2018
[8] Nitesh Funde and PardhiP. R. Analysis of Possible Attack on AODV Protocol in MANET.2014
[9] Neema Raza et al, Mobile Ad - Hoc Networks Applicationsand Its Challenges.2016
[10] Tanweer Alam and Baba Rababah, Convergence of MANET in Communication among Smart Devicesin IoT.2019
[11] Eduardo Soares et al, Experimentation with MANETs of Smartphones.2017
[12] Russell Skagg - Schellenberg et al, Performance Evaluation and Analysis of MANET protocols at Varied Speeds
[13] Govan Kadir et al, SMPR: A Smartphone Based MANET UsingPrime Numbers to Enhance the Network - nodesreachability and Security of Routing Protocols
[14] Tanweer Alam and Mohamed Benaida, The Role of Cloud - MANET Framework in theInternet of Things (IoT).2018
[15] Parul Gupta, A literature survey of MANET.2016
[16] Sadiya Mirza and Sana Zeba Bakshi, Introduction to MANET.2018
[17] Elmar Gerhards - Padilla et al, Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs.2007