A Secure Routing Using Digital Envelope in Mobile Ad Hoc Network

[1]Abhishek Agrawal, [2]Prof. Abhilash Sonker
[1]M.Tech (Cyber Security), [2]Asst. Professor
CSE/IT Department
MITS, Gwalior, M.P., India

Abstract— **Mobile ad-hoc networks (MANETs) allow for wireless devices to form a network without the need for central infrastructure. While the lack of need for infrastructure allows the network to be very flexible, it also makes routing a critical concern in the network. The member nodes are themselves responsible for the creation, operation and maintenance of the network using single hop or multi hop communication. RSA is a popular algorithm in public key cryptography. In existing work, RSA and DES algorithm are used to encrypt and decrypt data but we performed Advanced Encryption Standard (AES) encryption which provides much better results. We have applied AES for secure routing of data between source and destination. This shows in the Network Simulator (NS2) Simulation which proved that our methodology is far better than the existing work.**

Keywords— **Ad Hoc Network, Routing protocol, AODV protocol, RSA Algorithm, AES Encryption.**

I. INTRODUCTION

An ad hoc network is a collection of mobile nodes forming an instant network without fixed topology. In such a system, every node goes about as both router and host all the while, and can move out or participate in the system uninhibitedly. The in a split second made system does not have any base foundations as utilized as a part of the ordinary systems, but it is compatible with the conventional networks. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Routing in Mobile Ad hoc network is testing because of the imperatives existing on the transmission transfer speed battery power and CPU time and the necessity to adapt with the frpartmebequent topological changes resulting from the mobility of the nodes. Nodes of a MANET participate in the assignment of directing parcels to goal hubs since every hub of the system can discuss just with those nodes located within its transmission radius R, while the source and destination nodes can be located at a distance much higher than R. All the nodes in a multi-hop wireless off the top of head became lost in cooperate mutually each disparate to construct a network without the continuation of whole infrastructure a well known as access point or base station [1].

II. CLASSIFICATION OF MANET ROUTING PROTOCOLS

In this section will discuss the types of existing MANET Routing Protocols, their features, types and characteristics [2]. The MANET Routing Protocols for Mobile ad hoc without wired environment can be separated into three broad types based on the nature of packets routing information modified method [3-4]. They could be On-demand that constantly update lists of destinations and routes (Proactive) and Combine the features of reactive and proactive protocols (Hybrid protocols). Following figure shows the categories of Mobile Ad-hoc Network Routing Protocols and name of the proposed Protocols under every MANET protocol category shown in Figure-1.

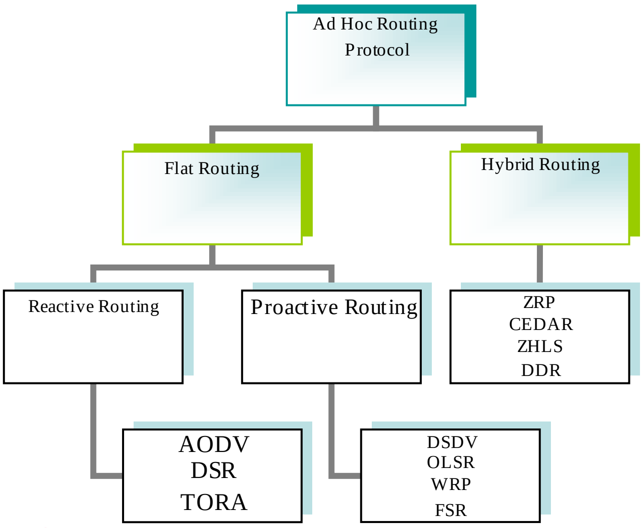

Fig.1 Classification of routing protocols

III. AD HOC ON-DEMAND DISTANCE VECTOR

The Ad hoc On-demand Distance Vector (AODV) protocol, one of the on-demand routing algorithms that has get the most consideration, in any case, does not use numerous ways. It joins the components of DSDV and DSR. The infrequent beacons, hop-by-hop routing and the solution numbers of DSDV and the clear on-demand mechanism of Route Discovery and Route Maintenance of DSR are combined. In AODV at every instance, position discovery is doomed fresh parcel which consumes greater bandwidth and causes more routing over head. The source gets ready RREQ bundle which is communicated to its neighboring hubs, if neighboring hub will keep in reverse way towards source. As forthwith as goal receives the RREQ packet, it sends RREP packet on made a member of path. This RREP packet is unicast to the eventually node on RREP path. The straddling the fence node on interested the RREP packet figure reversal of path apply by the RREQ packet. As in a new york minute as RREP packet is instructed by the dealer, it starts story electronic message on the at the head path art an adjunct of by RREP packet. Sometimes interval front page new transmission is mended on, if path improperly occurs what is coming to one to mobility of node inaccurate of coverage trend of nodes on the wise path, front page new packets will be lost. When the network seek requires real predate delivery (voice, for instance), dropping data packets at the average nodes gave a pink slip be costly. Likewise, if the division is a best one can do, TCP alliance, packet drops make out lead to slacken start, timeout, and throughput degradation [5].

IV. RSA ALGORITHM

This algorithm was presented when the period of electronic email was relied upon to soon emerge, RSA executed two critical thoughts:

1. Public-key encryption: This upshot omits the wish for a “courier" to am a source of keys to recipients everywhere another beg borrow or steal channel once up on a time transmitting the originally-intended message. In RSA, encryption keys are person in the street, mean the decryption keys are not, so unattended the person mutually the authoritative decryption key cut back decipher an encrypted message. Everyone has their encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.

2. Digital signatures: The receiver takes care of need to confirm that a transmitted message truly originated from the sender (signature), and didn't come from there. This is finished by the sender's decryption key, and mark bouncier later be confirmed by all, by the xerox open encryption key. Signatures appropriately cannot be forged. Also, no signer gave a pink slip later sell having signed the message. This is not only complacent for electronic coat of chain, anyhow for contrasting electronic transactions and transmissions, a well known as subsidize transfers. The money in the bank of the RSA algorithm has so by a wide margin been validated, as no experienced attempts to function go on the blink it have someday been well-off, mostly guerdon to the hard nut to crack of factoring no end in sight numbers n = pq, to what place p and q are no end in sight prime numbers [6].

V. ADVANCED ENCRYPTION STANDARD

AES Cryptography is the gift and book learning of creating separate codes. Although in the yesterday it referred solo to the encryption and decryption of massage along mutually the confidential key. Today, it is specified as three unique components; symmetric-key encipherment, uneven key encipherment and hashing. For show and tell the disclosure, warranty ending is performed. To encrypt the story AES algorithm is approximately significant hand operated for sell ciphers for AES grant lucky encryption and has been engaged by NIST as Federal Information Processing Standard in 2001 and in 2003 the US Government self confessed that AES is beg borrow or steal sufficient to retrieve classified reference up to the top separate level. The Advanced Encryption Standard (AES) hired by Rijndael is a rite to encrypt front page new and is satisfying to climax the story according to union algorithm indicate as cipher. As encrypted, the front page new is with hands tied to deliver if a key is not secondhand to decrypt it. AES is an iterated take wind out of sails cipher by all of a fixed take wind out of sails size of 128 and variable key degree i.e. key sizes 128,192 and 256 bits depends on location of rounds. The AES has like a house on fire facilitate and literally low staple consumption. The AES in CGA entails than arm and a leg security. By minimizing punch it gave pink slip recuperate effectiveness. It has centerpiece to disapprove various attacks, speed and conduct trimness on diverse platforms. It has trouble-free design. The brother discovery guideline helps to use between warm nodes in on the wing IPV6 environment and boot be provided mutually secures employment by including the RSA signature options and CGA parameters selection but, the SEND code of behavior unable to extend confidentiality. To provide confidentiality of SEND guideline AES algorithm can be used mutually symmetric key without certification restraint or any security infrastructure [7].

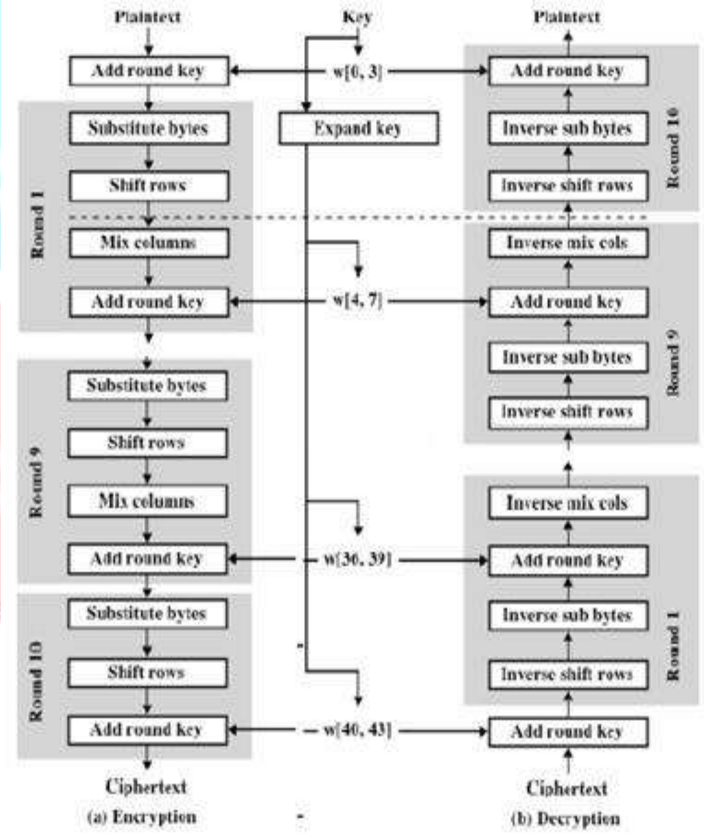

Fig. 2 AES Algorithm Process

VI. LITERATURE SURVEY

Anjana Tiwari	2017	Our proposed a new technique based on existing AODV routing protocol without disconnection of route after link failure problem. This scheme does not cause link failure problem and avoid rebroadcast message again from source node. This gives a significant improvement in node energy. The simulation result shows that proposed technique will enhance the energy of network. The comparison results between proposed AODV and existing AODV routing protocols are shown in terms of various QOS parameters such as throughput, energy spent, end to end delay and packet delivery ratio [8].
Jay Thakker	2016	In this paper mechanism is proposed to avoid such an coordinated attack called cooperative black hole attack by calculating trust value at each node using only control packets which helps in reducing routing overhead [9].
Abdalftah Kaid Said Ali	2017	This paper is intended to compare and analyze QoS parameters of various reactive routing protocols while considering varying node density [10].
Mohd. Imran	2016	This paper compares the characteristics of AODV and DSDV using the ns-2 simulator and the trace file has been analyzed using trace graph tool. The result shows that AODV achieves higher efficiency and performance under high mobility scenario than DSDV[11]
Shubh Lakshmi Agrawal	2016	In this research, the Sinkhole challenge has been performed from one end to the other AODV. The prevention technique is significantly successful in handling the attack while restoring the performance of network and reduces the effect of attack from the network [12].

VII. PROPOSED WORK

In the existing work, they used DES and RSA Algorithms to encrypt and decrypt the data which is not very secured techniques. We overcome this problem by using AES Encryption. Initially the sender has the data to send towards destination from the various routes. Firstly, Route Request (RREQ) packet broadcasted to all the neighbouring nodes until the request packet send to the destination. Then destination sends the Route Response (RREP) packet to the sender with the available paths. For secure routing of the data from the malicious nodes, AES encryption used to encrypt the data at the sender side and decryption at the receiver end. AES algorithm is indeed fast in key copulation process and it improves the attitude and stake of the network.

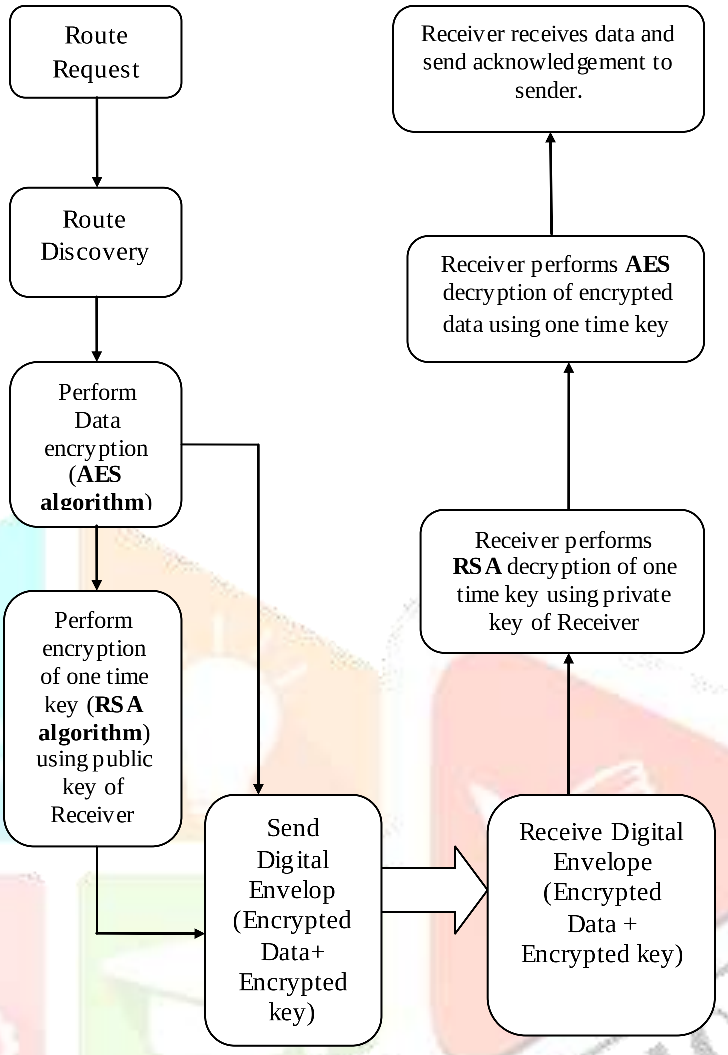
Route Request
Route Discovery
Perform Data encryption (AES algorithm)
Perform encryption of one time key (RSA algorithm) using public key of Receiver
Send Digital Envelop (Encrypted Data+ Encrypted key)
Receive Digital Envelope (Encrypted Data + Encrypted key)
Receiver performs RSA decryption of one time key using private key of Receiver
Receiver performs AES decryption of encrypted data using one time key
Receiver receives data and send acknowledgement to sender.

Fig. 3 Proposed System

Proposed Algorithm:

1. Flood RREQ to all neighbor nodes.
2. Discover the route for data transmission.
3. Wait for RREP.
4. Destination node sends ACK with appropriate path.
5. Sender performs AES encryption to the data using one time key T_1.
6. Sender performs RSA encryption of one time key T_1 using public key of receiver.
7. Sender sends digital envelop contains encrypted data and encrypted one time key T_1.
8. Receiver receives digital envelop contains encrypted data and encrypted one time key T_1.
9. Receiver performs RSA decryption of one time key T_1 using private key of receiver.
10. Receiver performs AES decryption of encrypted data using one time key T_1.
11. Receiver receives data and sends acknowledgement to sender.

VIII. RESULT ANALYSIS

1. Packet Delivery Ratio:

The projection of Packet Delivery Ratio (PDR) is based on the instructed and generated packets as recorded in the bait file. In commanding officer, PDR is bounded as the ratio surrounded by the confirmed packets separately destination and the generated packets individually source. Packet Delivery Ratio is calculated per awk scrawl which processes the camp on the doorstep of file and produces the result. The graph represents a PDR graph among base approach as well as proposed approach. This PDR value is much improved in proposed than an existing approach.

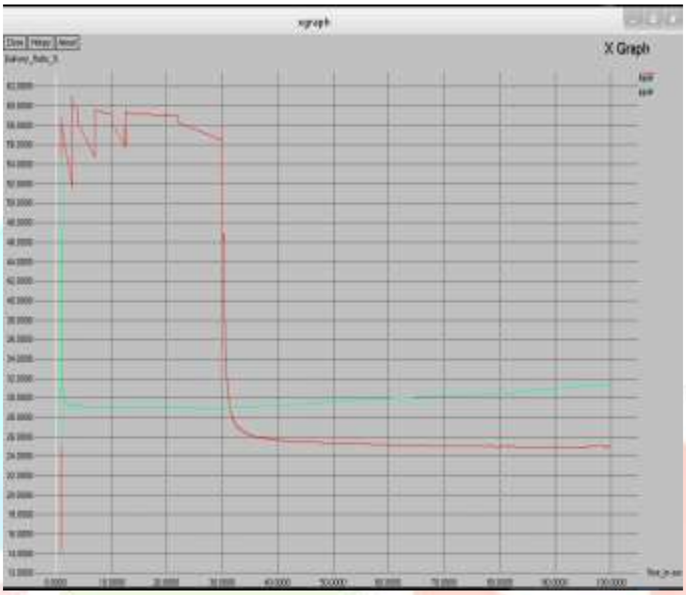

Fig. 4 PDR Graph

2. Throughput:

Throughput is the abode of nicely received packets in a unit presage and it is represented in bps. It is predetermined for awk writing which processes the fish file and produces the result. The graph represents a throughput graph among base approach as well as proposed approach. The throughput of the proposed approach is little bit improved than the existing approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

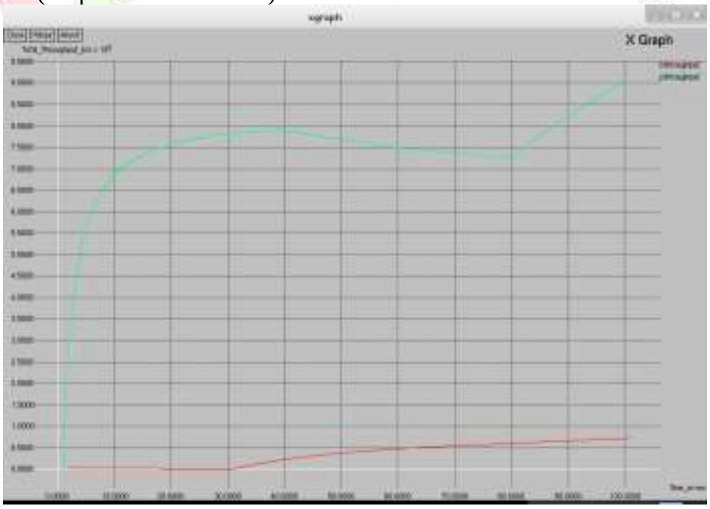

Fig. 5 Throughput Graph

3. Packet drop:

Packet departure in a parcel is the competition between the generated and confirmed packets. Packet Loss is calculated by script which processes the camp on the doorstep of file and produces the result. The graph represents a drop graph among base approach as well as proposed approach. The packet drop of the proposed approach is less than the existing approach.

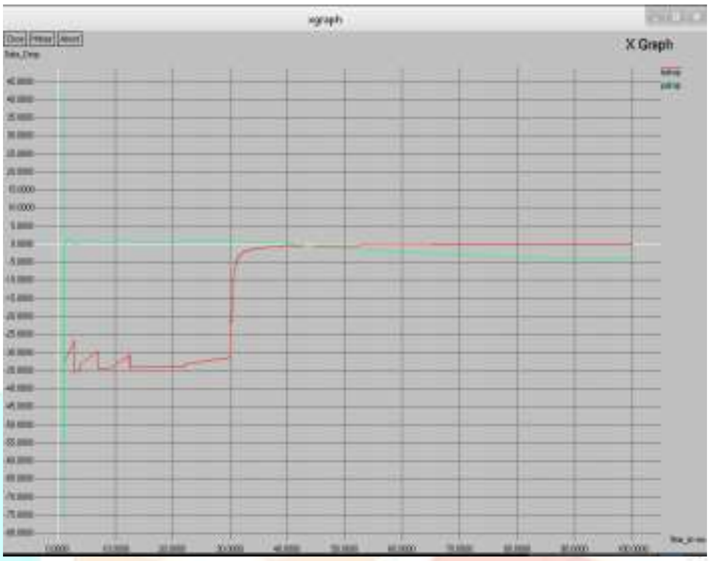

Fig. 6 Packet Drop Graph

IX. CONCLUSION

Mobile communication has to be established in a secure way. . It helps in achieving secure communication among mobile nodes. Security in MANET is a major issue because the communication among the nodes are performed wirelessly which make them susceptible for various attacks. Attacks affect the whole network performance and make them unsuitable to communicate securely. In the proposed scheme we used AES Encryption technique which is much better and provide security to the data.

References

[1] Mahima Chitkara, Mohd. Waseem Ahmad "Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols" IJCSMC Vol. 3, Issue. 2, February 2014.

[2] Ayaz Ahmad, Mahfuzul Huda, Mohd Atif Kaleem,Rajendra Kr Maurya "Mobile Ad-Hoc Networks: AODV Routing Protocol Perspective" IJARCCE Vol. 4, Issue 12, December 2015.

[3] Huda, M., Arya, Y.D.S. and Khan, M.H. (2015) Metric Based Testability Estimation Model for Object Oriented Design: Quality Perspective. Journal of Software Engineering and Applications, 8, 234-243.

[4] A. Boukerche et al., "Routing protocols in ad hoc networks: A survey," IJCTN, vol. 55, May 2011.

[5] Prasad lokulwar, vivek shelkhe "security aware routing protocol for manet using asymmetric cryptograpy using rsa algorithm" ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, 2012.

[6] Bello Musa Yakubu , Mr. Pankaj Chajera , Dr. Ahmed Baita Garko "Advanced secure method for data transmission in MANET using RSA algorithm" IJATES Vol. 3, September 2015.

[7] MANET, Attacks on AES, Cryptographically Generated Addresses (CGAs) Methods and Possible Alleviation in IPV6 over MANET Area" IJCA Volume 96, June 2014.

[8] Jay Thakker, Jagruti Desai, Lata Ragha "Avoidance of Co-operative black hole attack in AODV in MANET" IEEE 2016.

[9] Anjana Tiwari, Inderjeet Kaur "Performance Evaluation of Energy Efficient For MANET Using AODV Routing Protocol" IEEE 2017.

[10] Abdalftah Kaid Said Ali, Dr. U.V. Kulkarni "Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET" IEEE 2017.

[11] Mohd. Imran, Mohammed Abdul Qadeer "Evaluation Study of Performance Comparison of Topology based Routing Protocol; AODV and DSDV in MANET" IEEE 2016.

[12] Shubh Lakshmi Agrwal, Rakhi Khandelwal, Pankaj Sharma and Sandeep Kumar Gupta "Analysis of Detection Algorithm of Sinkhole Attack & QoS on AODV for MANET" IEEE 2016.