IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 11-14

Comparison of AODV and M-AODV IN MANET

K.Thamizhmaran
Assistant Professor in ECE, Department of Electronics and Communication Engineering, FEAT, Annamalai University

Abstract: *Mobile Ad hoc Network (MANET) is the significant technology among various wireless communication technologies where all the nodes are mobile and which can be connected to dynamically used wireless link in a random manner. The self-configuring ability of nodes in MANETs made it popular among critical applications like military use or natural emergency recovery. Most of the proposed protocols assume that all nodes in the network are cooperative, and do not address any security issue. To adjust to such trend, it is vital to address its potential security issues. The main objective of this paper is to define the path for security and to further improve delay, energy, throughput, routing overhead, packet delivery ratio and at the same time to create energy enhanced way with excellent security. In this paper, performance analysis ofModifiedAd hoc On-Demand Distance Vector(M-AODV) designed for MANET. In this scheme create faster, smaller, and more energetic and efficient cryptography. Network Simulator (NS2) is used to implement and test the proposed system. The proposed cryptography provides secured transmission, further it reduces routing overhead, improves packet delivery ratio and throughput.*

Keywords: *Mobile ad-hoc networks, Routing, AODV, M-AODV, NS2.*

I. INTRODUCTION

The mobile nodes that are in the radio range of each other can directly communicate, whereas others need the aid of intermediate linked nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully dynamically distributed, and can work at any place without the help of any fixed infrastructure as base stations. MANET suffers from a great efficiency loss due to the misbehaving nodes which may be constrained by the resources as battery power and bandwidth of topology. Different approaches have already been proposed to detect and prevent the misbehaviour in MANET.

Routing protocol

A static routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two active nodes on a computer network. Routing algorithms determine the specific choice of route. Each router only has a prior knowledge of networks attached to it directly. Routing protocols share this information among other immediate neighbors, and then whole network. The two main types of routing are static routing and dynamic routing. The entire router learns about remote networks from neighbor routers or from an administrator and builds an update routing table. If the network is directly connected, then the router already knows how to get to the network. The router learns how to get to the remote network with either static or dynamic routing. If static routing is used, then the administrator has to change all routers in the network and therefore no routing protocol is used: Only Dynamic Routing Protocol (DSR) uses routing, which enables routers. Generally, there are two different stages in routing: they are route discovery and forwarding data packets. In route discovery, the route to a destination will be discovered by broadcasting the query. Then, once the un-breakable route has been established, data forwarding will be initiated and sent through the routes that have been determined. The power consumption, route relaying load, battery life, and reduction in the frequency and bandwidth of sending control messages, optimization of size of headers and efficient active route reconfiguration should be considered when developing a routing protocol.

II. LITERATURE SURVEY

An elliptic curve cryptography (ECC) cipher suite for transport layer security was completed by S. Blake-Wilson et al An acknowledgment-based approach for the detection of routing misbehaviour in MANETs was done by Balakrishnan et al Bits security of the elliptic curve Diffie-Hellman secret keys were displayed by D. Jetchev et al Design of a new security protocol using hybrid cryptography algorithms was discussed by S. Subasree et al Public keys were found by A. K. Lenstra et al Yi-an Huang and Wenke Lee, approach is proposed to detect and isolate the misbehaving nodes. In this approach cluster-based detection method is used to address the run-time resource constraint problem. Bounpadithkannhavong et al, Proposed a method in which a survey of routing attacks in mobile ad hoc networks to define the current state of the routing attack and countermeasures.

III. PROPOSED SYSTEM

Elliptical curve cryptography

The method for obtaining public and private keys has generated considerable interest since key sizes can be made very smaller (in bits) while offering the same level of security algorithm. The smaller key size also implies much lower processing and power requirements for encryption and decryption of each data. Elliptic curve cryptography system, whose security rests on the discrete algorithm problem over the points on elliptic curve. ECC hybrid cryptography can be used to provide both an encryption scheme and a decryption scheme. The elliptic curve cryptography discrete algorithm problem can be stated as a prime p and an elliptic curve xP.

Mathematical details of implementation

When setting up an elliptic curve cryptography system, there are three basic decisions that need to be made in the selection of

- The underlying finite field Fp.
- The representation for the elements of Fp.
- The elliptic curve E over Fp.
- The curve point.

Key exchange

The purpose of the Diffie-Hellman key exchange is to generate a point, which will act as an elliptical key algorithm for a classic cryptography system. The public key cryptography is used only to exchange key and subsequently conventional cryptography is used. The key exchange procedure in ECC is as follows. Suppose 2 persons, X and Y, need to communicate via system, a key is exchanged secretly between X and Y and further communication takes place using conventional cryptosystem.

Encryption and decryption

a) System entities

- A Galois finite field GF is elliptical curve cryptosystem P (x) with an access point P lying in GF.
- Zp denotes the order of P.
- GF, P (A), P and Zp are made public key.

b) Secret key generation

- Generate a random number k, Zp-1
- Compute Q=KP.
- Point Q is made Public.
- K is made private or secret key.

c) Encryption process (Suppose X sends a message m to Y)

- Look up B's Public Key: Q.
- Represent the TX message 'm' as a pair of the field elements (m1, m2), m1 GF, m2 Zp-1.
- Select a random integer, such that Zp-1
- Compute the point (A1, B1) = P
- Compute the point (A2, B2) = Q.
- Combine both the field elements m1, m2 with A2, and B2 with an algorithm to give two field elements c1 and c2.
- Transmit the data m = (A1, B1, c1, c2) to Bob.

d) Decryption process (B gets the text m = (A1, B1, c1, c2) from A)

- Compute the point (A2, B2) = k (A1, B1), using its private key k.
- Decrypt m1 and m2 from m. The prime p used in the ECC hybrid system can be smaller than the numbers required in all the other types of cryptograms, so another advantage of the ECC is that the modified calculations required are carried out over a smaller modified operation. This leads to a significant improvement in efficiency in the operation of the ECC over both integral factorization and discrete algorithm cryptograms.

IV. METHODOLOGY

Elliptical hybrid cryptography Symmetric key ciphers are significantly faster than asymmetric ciphers, but require all parties to somehow share a secret (the key). The asymmetric key algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. The message itself is then encrypted using the symmetric key cipher and the secret key. Both the encrypted secret key and the encrypted secure message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own plane private key, and then uses that key to decrypt the message. Elliptical cryptographic algorithms are used with a view to obtain the merits of the systems. The method should be completely secure. The encryption / decryption cryptography process should not take longer time. The generated cipher text should be compact in size. The key exchange problem should be solved by the new method.

Simulation configurations

To facilitate the comparison of the simulation results with other research works, the default scenario setting in NS 2.34 has been adopted. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the non-wired extension of NS2, where the total bits transmitted is calculated using application layer data packets only and total energy.

Table 1. Simulation parameter

Parameter	Values
Examined protocol	M-AODV
Application traffic	CBR
Transmission range	800m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	700s
Number of nodes	100
Area	800 x 800m

V. RESULTS AND DISCUSSIONS

In this paper discuss M-AODV and AODV with follow above simulation parameters.

Table 2 packet delivery ratio

RP / NN	30	60	90	120	150
AODV	0.86	0.82	0.73	0.68	0.66
M-AODV	0.92	0.86	0.77	0.72	0.70

From Table 2, it is clear that secure proposed scheme M-AODV surpasses AODV performance by above 70% when there are 20 and 100 nodes in the network.

Table 3 routing over head

RP / NN	30	60	90	120	150
AODV	0.15	0.28	0.35	0.44	0.58
M-AODV	0.12	0.25	0.32	0.40	0.55

Simulation results of routing overhead shown in Table 3. It is clear that M-AODV has the lowest overhead of about 20 to 100 number of nodes.

Table 4 throughput

RP / NN	30	60	90	120	150
AODV	0.15	0.27	0.40	0.53	0.57
M-AODV	0.25	0.37	0.50	0.63	0.68

Table 4 proves that the proposed M-AODV provides better performance of the throughput when there are 20 to 100 of nodes compared to AODV routing protocol.

Table 5 remaining energy

RP / NN	30	60	90	120	150
AODV	0.92	0.84	0.76	0.72	0.64
M-AODV	0.95	0.89	0.80	0.76	0.70

Table 4 clearly show that the proposed M-AODV increases the remaining energy with increasing number of nodes from 20 to 100 compared to AODV.

Table 6 end-to-end delay

RP / NN	30	60	90	120	150
AODV	0.17	0.23	0.29	0.38	0.47
M-AODV	0.12	0.18	0.24	0.33	0.42

According to table 5, it is clear that proposed scheme M-AODV surpassed the performance of AODV in minimising end-to-end delay by 5% when there are 20 to 100 nodes in the network. As the proposed algorithm finds different short routes frequently, it is possible to minimize the delay.

From all the above figures and tables, it is clear that the comparison of the M-AODV illustrate that the proposed algorithm outperforms the AODV by providing lowest end-to-end delay, packet drop and routing overhead with increase in the number of nodes.

VI. CONCLUSION AND FUTURE WORK

Packet-dropping and loss attack have always been a major threat to the security in MANETs. In this research paper, a novel approach named M-AODV protocol specially designed for MANETs is proposed in comparison with other popular techniques in different scenarios through simulations. The results demonstrated positive performance of the remaining energy in M-AODV than, the researchwas extended to incorporate elliptical curve cryptography in this proposed scheme. Although it generates more end-to-end delay in some cases, as demonstrated in this research, it can vastly improve the network's PDR to more than 1.5% compared to the existing AODV routing protocol and improve remaining energy by 6% compared to the existing AODV routing protocol when the attackers are smart enough to forge acknowledgment packets.

REFERENCES

[1]. Parma Nand, Sharma (2011) "Routing Load Analysis of Broadcast based Reactive Routing Protocols AODV, DSR and DYMO for MANET", IJGDC.

[2]. Ade and Tijare (2010) "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-hoc Networks", IJITKM, Vol. 2, No. 2, pp. 545-548.

[3]. Johansson, et al. (1999) "Scenario based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks", IEEE.

[4]. Marti, et al. (2000) "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", ACM, 2000.

[5]. Pushpalatha, et al. (2009) "Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad-hoc Networks", World Academy of Science.

[6]. Pirzada, et al. (2005) "Secure routing with the AODV protocol", IEEE.

[7]. SemihDokurer, ErtenAcar, (2007) "Performance Analysis of Ad-hoc Networks Under Selective Black hole Attacks", IEEE, pp.148-153.

[8]. Kannhavong, et al. (2007) "A survey of routing attacks in mobile ad hoc networks." IEEE, Vol. 14, No. 5, pp. 85-91.

[9]. Komninos, et al. (2007). "Detecting unauthorized and compromised nodes in Mobile Ad-hoc Networks". Elsevier, Vol. 5, pp. 289-298

[10]. Nidal Nasser and Yunfeng Chen (2007) "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks", IEEE.

[11]. Balakrishna, et al. (2007) An Acknowledgment-based Approach for the Detection of Routing Misbehaviour in MANETs,*IEEE Conference*. pp. 1-35.

[12]. Blake-Wilson S. et al. (2006) Elliptic curve cryptography (ECC) cipher suites for transport layer security,*TLS. RFC 4492*, pp. 1-32.

[13]. Jetchev D. et al. (2008) Bits security of the elliptic curve Diffie-Hellman secret keys,*Springer*,Vol. 5, Issue. 15,pp. 75-92.

[14]. Subasree S. et al. (2010) Design of a New Security Protocol Using Hybrid Cryptography Algorithms,*IJRRAS*, Vol. 2, Issue. 2,pp. 95-103.

Biography:

K. Thamizhmaran received his BE and ME from Annamalai University, Tamilnadu, India in 2008 and 2012, respectively. He is currently working as an Assistant Professor of ECE in the Department of Electronics and Communication Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu, India. His research interest includes networks security, ad-hoc networks, mobile communications, and digital signal processing. He has published more than 89 technical papers at various national / international conferences and in journals. He is a life member of IAENG and IACSIT.