International Journal of Engineering &Technology, *7 (3.12) (2018) 621-626*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Enhanced Reactive Routing Protocol for Manet Using Two Fish Algorithm

M.Deepa[1], P. Krishna Priya[2]

[1]Ph.D Scholar, [2]Director, [1,2]Department of Computer Applications,
Coimbatore Institute of Management and Technology, Tamil Nadu, India.
**Corresponding Author Email: [1]deepshini21@gmail.com*

Abstract

In Mobile Adhoc Network (MANET) implementing a secure communication is a critical task due to its nature of wireless, infrastructureless, arbitrary network. Its not organized by any centralized control. Each node in this network acts as a router. Routing plays a major role in the network data transmission. Various protocols exist for the purpose of routing process. On Demand routing is a category of routing protocol were routes are obtained only on demand. AODV is one of the efficient on demand routing protocol. In this work an enhanced protocol with security features, the Secure AODV- ESB (Secure Adhoc On Demand Distance Vector based on Energy level and Signal Strength Implementing Bayesian Probability) has been proposed for Mobile Adhoc Network. Its is an extension of the previous work AODV – ESB protocol, which is a modification of the existing AODV protocol. The AODV protocol works on two phases. The route discovery process and route maintenance phase. Major problem faced by AODV was the frequent route break caused by the dynamic mobile nature of the Mobile Adhoc network, which leads to frequent route discovery process. To avoid frequent route break AODV-ESB routing protocol was proposed, it adopts the energy level and Signal strength as parameters for the route selection for transmission of data. Bayesian probability implementation in the protocol increases the chance of adopting more reliable and optimized path. Another major issue in data transmission in the Adhoc network is the security. Securing data from access of the unauthorized person is a major responsibility of the protocol. This new secure AODV- ESB protocol protects against attackers by identifying the malicious node and eliminating them and also secures data by implementing cryptography using Two Fish Algorithm. This ensures secure data transmission in MANET more efficiently than the original AODV protocol. Analysis using the NS 2 Simulator proves that Secure AODV- ESB performs better than the previous work AODV- ESB.

Keywords: *Mobile Adhoc Network (MANET), AODV protocol, Network Simulator (NS 2), Bayesian Probability, Two Fish Algorithm.*

1. Introduction

The Mobile Adhoc Networks (MANET) is an autonomous system of wireless, infrastructureless network with dynamic topology [1]. In MANET each node plays the role of router. Routing process plays a major role in the adhoc networks. An efficient protocol provides a greater data transmission and minimum delay [2]. Adhoc Network means a network for particular special purpose, which implied in case of military communication, emergency disaster or rescue operations. These networks are challenged by severe security threats due to the vulnerability in the design. In these cases data transmission is to be done efficiently in a more secure manner. Each node in the network should be trust worthy [3][4]. Lots of researches are undertaken to provide a secure data transmission and number protocols are designed to face the attacks.

Routing attacks and data forwarding attacks are the two categories of attacks faced in MANET [5] [6]. Routing attacks can be defined as the action that performed, which does not follow the rules of the routing protocol. Propagating false route and disturbing the network is the main objective of the routing attacks. Target of the data forwarding attacks is to modify or drop the data packet without creating any distraction to routing protocol. Wireless network is accessible to both authorized nodes and attacker nodes and face the attacks in MANET. The role of the routing protocol is to act as the defender and impart secure data transmission. This can be succeeded by implementing the cryptographic algorithms and transmit data from source to destination.

A routing protocol is reliable for security if it has the capability of identifying trust worthy nodes and discovers a reliable and trustworthy route to transmit the data securely form the source node to the destination node. Adding security feature to a protocol in an efficient manner is by providing secure protocol with improved efficiency.

The rest of the paper is organized as follows. In section II, detailed reviews of the existing modified secure AODV protocols are presented. The Previous work, modification of AODV protocol, the AODV – ESB MANET routing protocol and characteristics of AODV –ESB protocol have been discussed and the problem that exist in AODV-ESB protocol is identified. In Section III the working principle of the AODV –ESB protocol in different phases are discussed in detail. Section IV discusses about the proposed secure AODV –ESB routing protocol and it explains how data is transmitted from the source to destination securely using cryptography algorithm and how the network is safe guarded from the malicious node. Section V presents the experiments carried out in NS-2 in MANET implying the proposed routing protocol secure AODV- ESB, using Two Fish algorithm for cryptography and proposed new algorithm to prevent from attack of malicious nodes. The Simulations performed to obtain the performance of the proposed algorithm with various scenarios having different interval, packet size and simulation time and the results are presented in this section. Section VI presents the conclusion of the study.

2. Related Work

In Mobile Adhoc Network security of transmitted data is unavoidable. Many researchers have worked on the security issues and proposed number of protocols. In MANET data transmission, routing plays a major role and security feature can be implemented in the routing phase which is processed in the network layer. Number of research publications have come out based on the security issue in MANET in the recent past years. The security level and efficiency of the protocols are evaluated based on different metrics by performing simulations with different modified secure protocols of MANET under various conditions and results are published. This paper addresses the problem of securing a modified AODV routing protocol AODV-ESB protocol.

In [6], the author presented a new protocol secure-AODV, a modified protocol of AODV, which uses the hashed message authentication algorithm. It provides fast message verification, message authentication and intermediate node authentication. Implying this method reduces the time delay and control packet overhead. In this method the message and message integrity services are provided by using authentication the pair wise shared secret key. The optimal route is selected depending on power level of the nodes and hop count. Its proved that it performs better than the base AODV protocol.

In [7], a security schema has been proposed by the author for AODV protocol. As per the schema each node while joining the network obtains a shared secret key. It also holds the list of the neighbor nodes. This security schema proposes to execute the authentication process with the sender before executing the route discovery steps in the protocol. The special feature of this protocol compared to other proposed security routing protocol is it requires less computation power.

In [8], the author has implemented an optimized AODV routing protocol SRPAODV. Paper proves SRP is more efficient and secure than the existing AODV protocol. This protocol has made use of the Blowfish cryptosystem for encryption and decryption of the transmitting data. Here encryption in source node and decryption in destination is performed.

In [10], the author proposes the protocol ARAN. This protocol detects and protects against malicious actions by third parties. It provides authentication, and message integrity. ARAN provides an increased security in minimal cost

3. AODV – Adhoc on Demand Distance Vector Routing Protocol

The Adhoc on Demand Distance Vector [AODV] routing protocol was developed based on the Destination Sequenced Distance Vector [DSDV] routing protocol [2]. DSDV was developed based on the Bellman-Ford routing mechanism. The DSDV protocol overcame the Looping problem that existed in the Bellman-ford protocol. DSDV is a table driven algorithm various AODV is an on demand basis routing protocol. The on demand basis route discovery policy minimizes the number of broadcast of AODV compared to the DSDV protocol.

The nodes of the Pure AODV protocol maintains only the details of the active paths and get involved in exchange of those routing table updates, inorder to get reduced of control overhead. AODV routing takes place in two phases, the route discovery phase and the route maintenance phase. Hop count is used as a metric for the route selection. Freshness of the route is observed by the sequence number.

When the source node requires sending the data packet it initiates a route discovery process. Source node broadcasts the RREQ packet to its neighboring nodes. If the neighboring node is not the destination the RREQ packet is further forwarded towards the destination through the intermediate nodes. When the RREQ reaches the destination, a RREP packet will be unicasted by the destination node to source node and the data transmission starts from source node to destination node through intermediate nodes.

A. AODV – ESB : A Modification of AODV Protocol

AODV - ESB protocol, a modification of the existing AODV protocol. The objective of this protocol is to overcome the major problem faced by the AODV protocol, the frequent route break, which will lead to frequent route discovery process and increases the number of control overhead. This will further result in reduced throughput, packet delivery ratio and increased control overhead and end to end delay.

Major issues that cause the route break are the node power failure and the loss of signal strength. These both issues are over come in the modified AODV- ESB protocol by selecting the optimized path based on the metric, the energy level and signal strength of the node. For more accurate and efficient optimization Bayesian Probability is implemented and achieved the goal of optimized AODV routing protocol.

B. Security Threats

Security mechanisms to safe guard against the attacks are not provided in the original AODV protocol [6]. There are some major weaknesses in the AODV protocol. A malicious node may impersonate a source node or destination node, decrease hop count in RREQ or RREP, increase sequence number in RREQ or RREP, which causes a check to the message integrity and consistency of the network. The routing attacks can also be done by sending false route error messages [10]. These security issues are not rectified in the optimized AODV – ESB routing protocol.

4. Secure Optimized AODV Protocol

The proposed Secure AODV – ESB protocol works in three phases.

- Neighbors Creation – Eliminating the Malicious Node
- Root Construction Implementing Bayesian Probability
- Secure Data transmission by Implementing Cryptography Algorithm – Two Fish Algorithm

The protocol monitors the network and periodically collects the network related data. Use this data to analyze and find the malicious nodes, eliminate them and enter the next phase. Taking energy level and Signal strength as metric and implementing the Bayesian probability the Optimized route is selected. After secure route selection the source node transmits data implementing the cryptography algorithm. The data is encrypted at the source node and decrypted in the destination node using the Two fish Algorithm.

A. Neighbors Creation – Eliminating the Malicious Node

In this phase the protocol monitors the network activities and Collects network related data periodically. The node maintains network link table and a result table. Network link table holds the RREP, RREQ and RERR values. Result table holds the control packet counts, Loss packets and Percentage of packets received.

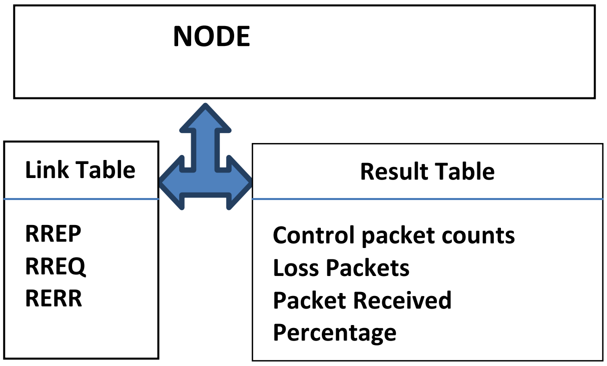

Fig. 1: Structure of Link table and Result Table Associated with Nodes

1. Initial Stage

In the Initial stage, both network link table and the result table are continuously updated with frequent time interval. The highest value from table is found. The results are obtained at every interval. Each node computes average of each table and updates its values. The initial node character is updated by these values.

2. Present Network Activities

Network link table is validated by the node to know presence of any attack. The probability estimation of network link values are received and updated. At each time, the proposition for each value of network link table is computed by the node. If proposition not computed by any node, its assumed that attacker's present in that time period. Then initial stage values with weight value are computed which stands for projected and experimental changes. The updated values reflect the present character of the network. Once an attack has been identified, then attacker is detected by policy. Each node computes self-assurance of the attack that has been detected. The severity of the network is obtained by estimating the result deprivation using the result table. Using this each node conveys about its neighbors self-assurance. On obtaining self-assurance, if detected as harmful, then all normal nodes decides about suitable penalty. Normal nodes decide to eliminate the node from network activities

In case, nature of harm is less then allows attacker to send data packets. On elimination of the attacker node, If no neighbor node is present nearby the Attacker node, then no possible routes will be available. To overcome the issue, when eliminating an attacker from the network, if any other node is not available nearby, then to avoid generating a communication hole, some other good node is made to move near the attacker position.

B. Root Construction Implementing Bayesian Probability

Optimal route selection is essential for efficient transmission of data from the source to the destination. Route selection is initiated with the new route discovery process which considers the energy level of the nodes and signal strength of the links as the criterion for the choosing the reliable path. During the data transmission the chances of link break are estimated in prior based on the energy level and signal strength of the nodes in the data transmitting path. On the route construction process the next node selection is made on the priority of the node with higher energy level and the signal strength of the link, which relies on the distance between the nodes which determines the radio range between nodes.

1. Bayesian Probability In Optimal Route Selection

The proposed protocol considers two metric parameters in optimal path selection. Estimating a best option when two piece of information are given can be achieved by usage of the Bayesian probability. Implementing Bayesian probability takes the node energy level and signal strength of links as the two selection metrics and predicts the more reliable path. Implementation of Bayesian probability results in reduced control overhead which simultaneously results in reduced node power and bandwidth usage providing a better performance of the network

2. Algorithm for Optimised Route Selection

Source node requires transmitting of the data to the destination node. It initiates the route discovery process. Generates the RREQ packet and broadcasts to its neighboring nodes. The further forwarding of the RREQ is depended on the energy level of the nodes and the signal strength of the link between the nodes. Since two piece of information is to be considered, the Bayesian probability is implemented to select the more optimal path. The RREQ packet is forwarded to limited number of nodes which satisfy the set criterion. The forwarding of the RREQ packet is carried on until it reaches a destination node or an intermediate node that contains the optimal path to the destination. The RREQ packet contains the destination ID and Destination sequence number. The freshness of the route is determined by the sequence number of the node.

The selection of the next node is done on the basis of two dimensional inputs the signal strength and the energy level. In each dimension the summation and mean value are estimated to find the difference between the input and mean parameter. Taking to consideration the summation of difference values and the number of entries entered in the next hop list the statistics values such as the deviation in terms of variance and standard deviation are computed. After the computation the optimal text move is selected for the transmission the packet.

The destination node on receiving the RREQ packet returns a RREP packet and forwards it towards the source node. On receiving the RREP packet the source node starts transmitting of the data packet. The RREQ packet and later the data packets are transmitted only on limited number of path resulting in reduced network control overhead, on effect to this the node energy and bandwidth consumption is reduced.

$$f(x) = x^{r-1} e^{-x} /[(r) \quad \text{--------} \qquad (1)$$

In each dimension the Gaussian distribution is derived from the Exponential probability which is shown in equation 1. The normalized distributed value of the node probability enables us to compute the probability of normal distribution. Gamma function enables exploring the gamma distribution. Gamma distribution probability is computed with the product of the probability with the exponential power including the gamma member function.

Alpha beta function is used to estimate the prior probability of the gamma function. The posterior probability is estimated from the learning rate and the alpha beta function. Finally the gamma probability is calculated using the likelihood function, where the likelihood function is the ratio of the posterior probability and prior probability. The contribution probability of each node is derived from the marginal probability of the gamma input dimension. In the routing process the next hop is determined on the basis of node with maximum contribution probability.

C. Secure Data Transmission by Implementing Cryptography Two fish Algorithm

Two Fish is a well-known encryption algorithm commonly used in cryptography and steganography. Two Fish algorithm is derived from Blowfish algorithm. Two Fish is a 128-bit block cipher that accepts a variable length key up to256 bits. The cipher is a 16-round Feistel network with an objective function made up of four key dependent 8-by-8 bit Sboxes, a fixed 4-by-4 maximum distance separable matrix, a pseudo Hadamard transform, bitwise rotations, and a carefully designed key schedule. The Two Fish algorithm is implemented to proposed protocol after the process of optimized root selection using the Bayesian probability. The data transmitted from the source node is encrypted using the two fish algorithm and again the data its decrypted by the algorithm at the destination node.

Thus using the proposed protocol the data is securely transmitted in the optimal path

5. Simulation Model

The Secure modified AODV protocol is evaluated using the NS2 Simulator. To perform the simulations and analyze the results of their findings the NS2 tool is widely used by the researchers. The efficiency of the protocols under different circumstances is analyzed by performing simulations. Number of nodes used for the simulation is 50.The simulations are performed by varying the Interval, Packet size and Simulation Time. From the obtained results the performance of the protocol is analyzed

A. Evaluation Parameters

The efficiency and performance of the protocol is analyzed and evaluated based on the parameters throughput, packet delivery ratio, end to end delay and goodput. Based on the above mentioned metric parameters the proposed protocol is compared with the existing AODV protocol

B. Simulation Environment

The MANET network Environment is dynamic one with frequent changing node position. The parameters of the simulation network can be altered and the efficiency of the protocol is obtained and analyzed based on the performance metrics. The Table 1 shows some of the simulation parameters.

Table 1: Simulation Parameters

S.No	Parameter Description	Value
1	Network Size	1000 m x 1000 m
2	Number of Nodes	50
3	Simulation Time	100,125,150,175,200
4	Antenna	Omni antenna
5	Radio Propagation Model	Two ray ground
6	Channel Type	Wireless Channel
7	Pause Time	0.1 sec
8	Packet Size	500,600,700,800,900,1000
9	Traffic Type	Constant Bit Rate CBR)
10	Data Transmission Agent	UDP
11	MAC Protocol	IEEE 802.11
12	Routing Protocol	AODV

C. Simulation Results

Simulations are carried on under various circumstances, as discussed in section IV by varying the network parameters and the results are obtained. Obtained results for the different parameter values of Secure ESB_AODV is compared with the previous work ESB_AODV, a modification of the AODV protocol. The resulted metric parameter values of AODV-ESB are compared and analyzed with the Secure AODV-ESB results. The result obtained proves that secure AODV-ESB performs better than the AODV-ESB protocol.

Scenario I: Evaluation Performed Over Different Interval

The throughput of the Secure AODV-ESB and AODV-ESB protocols are compared in the Fig. 3. The result shows that the secure AODV-ESB protocol has a higher throughput than the AODV-ESB protocol. When the interval is minimum the variation in throughput is higher. Fig.4 plots the packet delivery ratio, that shows that AODV-ESB provides a packet delivery ratio of 86% whereas the secure AODV-ESB protocol provides a ratio of 97.31.99%. Fig.5 compares the end to end delay for secure AODV-ESB its in a average of 0.56 and for AODV-ESB its 1.5%. Fig.6 depicts the good put ratio for Secure ESB –AODV, which has a 50% greater efficiency than the former AODV-ESB.

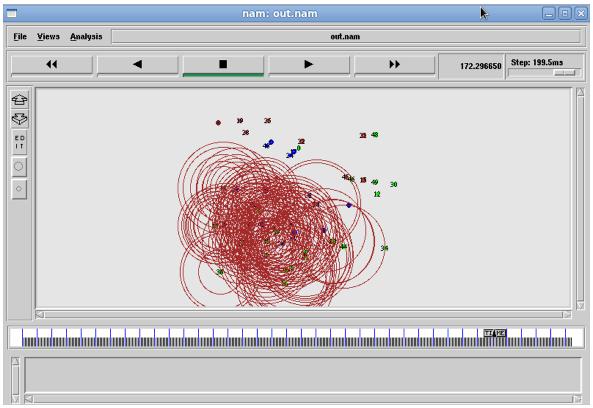

Fig. 2: Simulation Scenario Having 50 Nodes

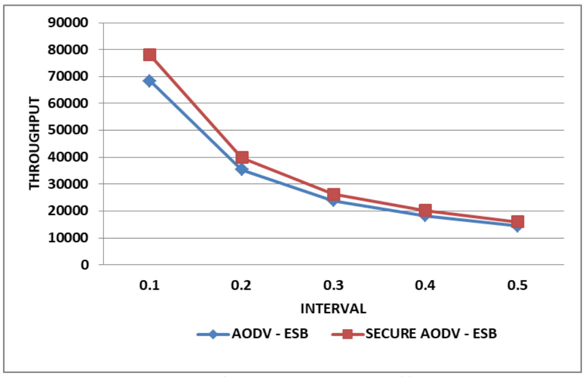

Fig. 3: Variation of Throughput with different Interval

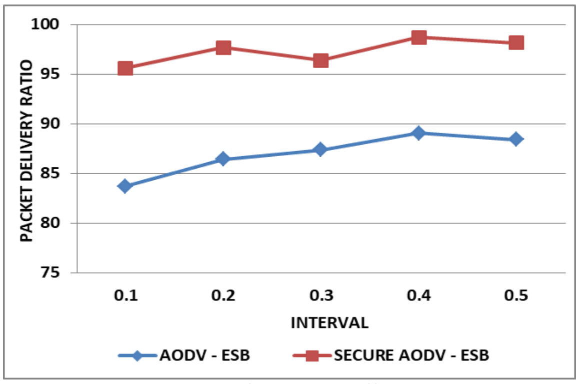

Fig. 4: Variation of PDR with different Interval

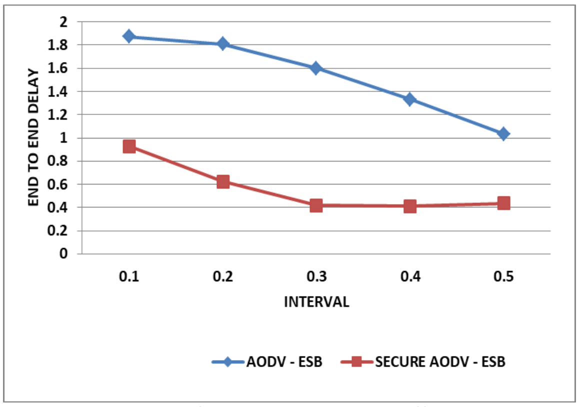

Fig. 5: Variation of end to end delay with different Interval

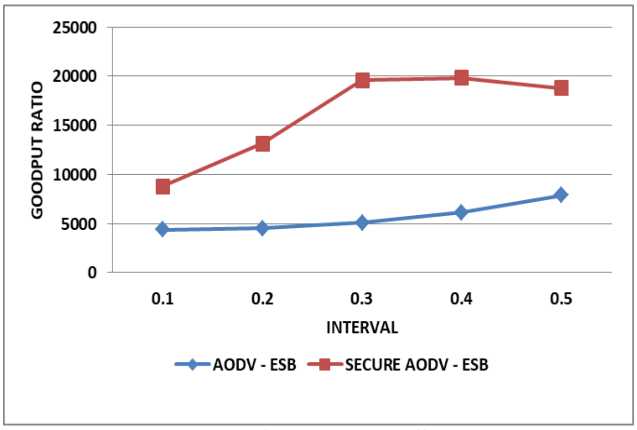

Fig. 6: Variation of Goodput with different Interval

Scenario II: Evaluation Performed by Varying the Packet size

Fig. 7 shows the fact that as packet size increases the throughput also increases for both protocol. With increase in packet size there is a uniform variation between the protocols. Throughout the process the proposed protocol has higher throughput compared to the AODV-ESB protocol. Fig. 8 shows that there is no variation in packet deliver ratio with variation in packet size Proposed protocol delivers an average of 84% while AODV-ESB delivers an average of 95% packet delivery ratio. With increase in packet size there is an increase in end to end delay in cases of both protocols. Secure AODV-ESB undergoes an average delay of 0.7 sec whereas AODV-ESB faces an average delay of 1.5 sec while varying the packet size. Fig. 10 depicts that there is variation in goodput with changes in the packet size.

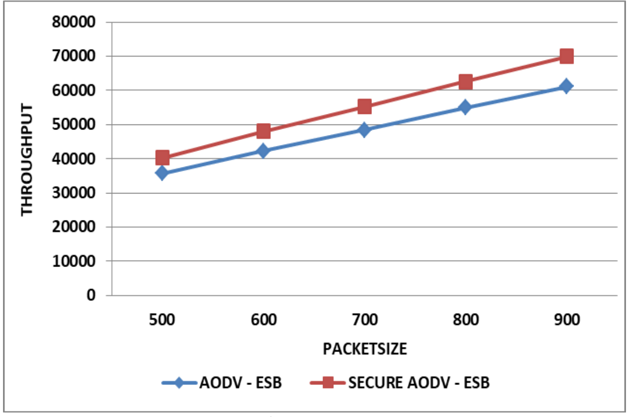

Fig. 7: Variation of Throughput with Packet size

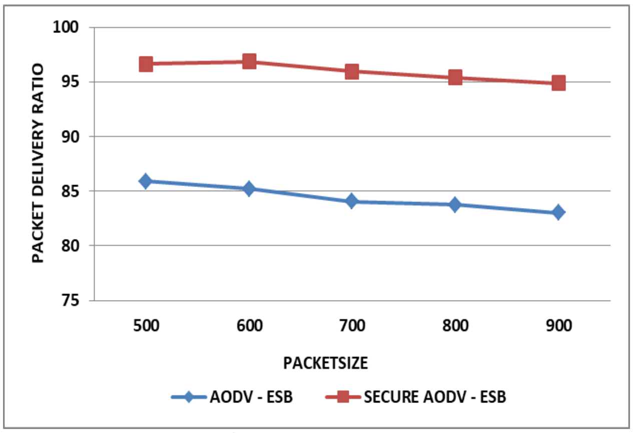

Fig. 8: Variation of Packet delivery ratio with Packet size

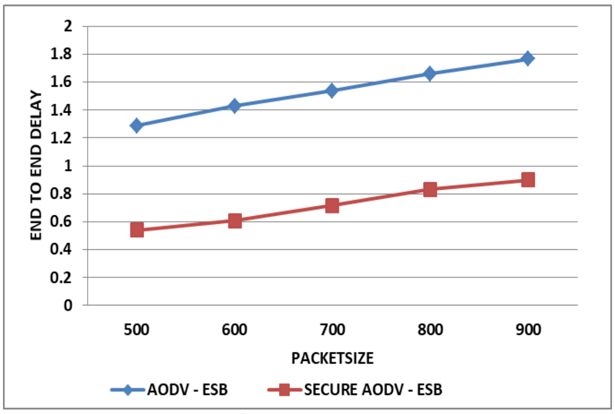

Fig. 9: Variation of end to end delay with Packet size

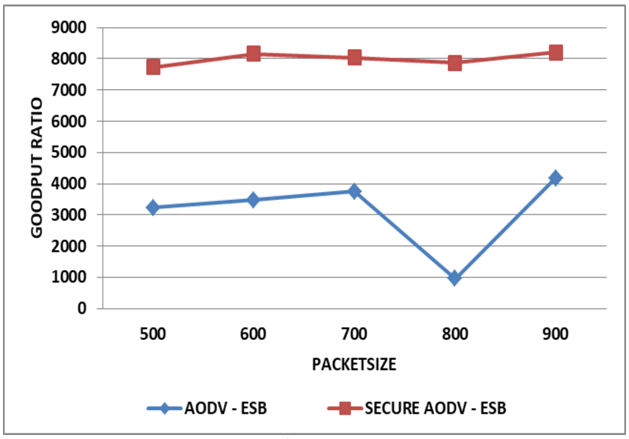

Fig. 10: Variation of Goodput with Packet Size

Scenario III: Evaluation Performed by Varying the Simulation Time

The Fig. 11 shows that proposed protocol has higher throughput compared to the AODV-ESB protocol. The proposed protocol throughput slightly decreases then maintains a constant throughput for all varying simulation timings. The AODV-ESB protocol maintains a constant throughput for all varying simulation times. The Fig. 12 shows a similar result for packet delivery ratio as that of the throughput. The Fig. 13 shows that there is a slight increase in end to end delay with increase in simulation time. Fig. 14 displays the goodput ratio of both protocols with varying simulation time. As in other cases the proposed protocol maintains higher goodput ratio compared to AODV-ESB, initially the value decreases but gradually increases and maintains a constant range of goodput ratio.

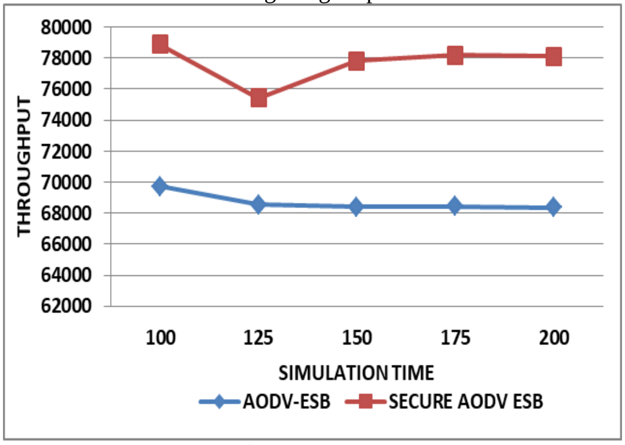

Fig. 11: Variation of Throughput with Simulation Time

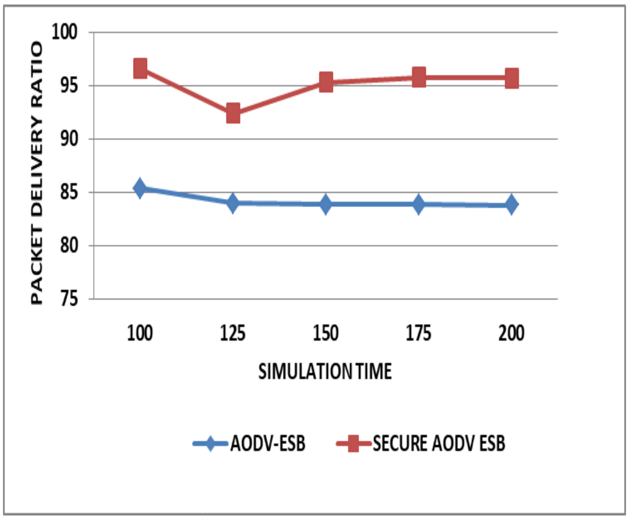

Fig. 12: Variation of Packet Delivery Ratio with Simulation Time

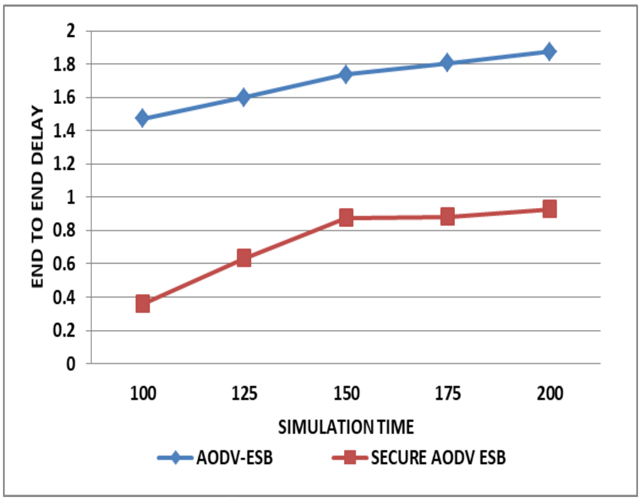

Fig. 13: Variation of End to End Delay with Simulation Time

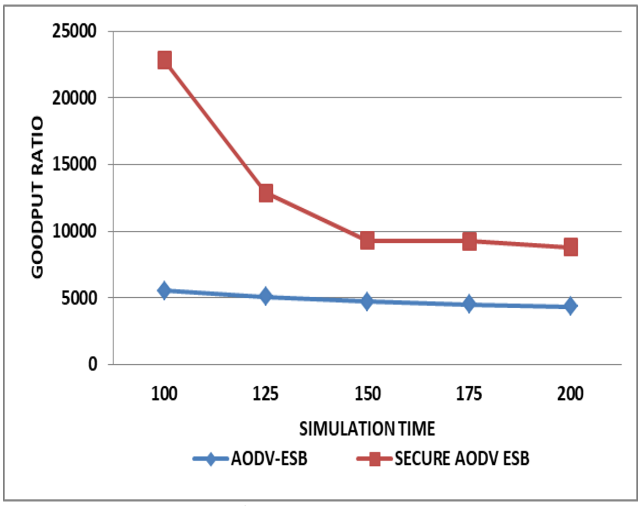

Fig. 14: Variation of Goodput Ratio with Simulation Time

6. Conclusion

The Mobile Adhoc Network is dedicated network used for particular purpose. Security is a major requirement of such network. As this environment is of wireless nature, all the communications are handled by the routing protocols. The efficient way of providing security in MANET environment is to make use of the secure routing protocols. In this paper we have proposd a secure Modified adhoc Ondemand Distance Vector protocol AODV-ESB. This protocol protects the MANET from attacks of malicious nodes.This on demand protocol provides secure transmssion of data from the source to destination using the Twofish algorithm.This protocolprovides an efficient secure routing in MANET.

References

[1] Lu Han, “Wireless Ad-hoc Networks”, Oct 8, 2004

[2] C. E. Perkins and E. M. Royer, ”Ad-hoc On-Demand Distance Vector Routing”, Proceedings of the 2nd IEEE, 2003

[3] K.Sivakumar, “Mobile Adhoc network routing principles and protocol evaluation metrics” , International journal of computer science and technology [IJCST], vol.2, no.4, pp-261-266,Oct-Dec.2011

[4] Bruce Schneier, John Kelsey, Dough Whiting, David Wagner, Chris Hall and Neil Ferguson, “Two fish: A 128 Bit Block Cipher”, Jun-1998.

[5] Morli Pandya, Ashish Kr. Shrivastava, “Review on security issues of AODV routing protocol for MANET“, IOSR journal of computer engineering, [IOSR-JCE], ISSN- 2278-8727, vol.14, no.5, pp-127-134, Sep-Oct.2013.

[6] Pabitra Mohan Khilar, ”Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism”, International journal of Network Security and Its Applications, vol.3, no.5, pp-230-240, Sep-2011.

[7] Phung Huu Phu, Myeongjae Yi and Myung – Kyun Kim, “Securing AODV Routing Protocol in Mobile Ad – Hoc Networks “, International Federation for Information Processing,LNCS 4388, pp. 182-187, 2009.

[8] Rizwan Akhtar, Noor Ul Amin, Imran Memon and Mohsin Shah. “Implementation of Secure AODV in MANET”, The International Society for Optical Engineering, vol.8768, Mar -2013.

[9] Vijaya Singh,Megha Jain, “Secure AODV Routing Protocols Based on Concept of Trust in MANETS”, International Journal of Advanced Research in Computer Engineering and Technology”, ISSN-2278-1323, vol. 3, no.12, pp. 4425-4428, Dec-2014.

[10] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M.Belding- Royer, “ A Secure Routing Protocol for AdHoc Networks“

[11] Bruce Schneier, Doug Whiting, “A Performance Comparison of the five AES Finalists ”, Apr– 2000.

[12] Nikita S.Karekar, Dr.R.S.Kawitkar, “ Security in Patient Data Communication using Encryption Algorithm”, International Journal of Innovative Research in Computer and Communication Engineering, ISSN-2320-9798,vol.5, no.5, pp. 9738-9745, May-2017.

[13] Aparna.K, Jyothi Solomon, Harini.M, Indhumathi.V,” A Study of Two Fish Algorithm”, International Journal of Engineering Development and Research, ISSN-2321- 9939, vol.4, no. 2,pp. 148-150, 2016.

[14] Mahsa Gharehkoolchian, A.M.Afshin Hemmatyar, Mohammad Izadi, “ Improving Security Issues in MANET AODV Routing Protocol “, Proceedings of International Conference on Ad Hoc Networks, pp. 237- 250, Nov- 2015 .