Indian Journal of Science and Technology, Vol 8(34), DOI: 10.17485/ijst/2015/v8i34/85243, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An ANN Approach in Ensuring CIA Triangle using an Energy based Secured Protocol E-AODV for Enhancing the Performance in MANETS

A. Sumathi* **and B. Vinayaga Sundaram**

Department of Information Technology, MIT Campus, Anna University, Chennai - 600025, Tamil Nadu, India; sumisolay@yahoo.com, bvsundaram@annauniv.edu

Abstract

Evaluating a routing protocol in MANETS is a difficult task due to mobility of nodes and decentralized administration. In Adhoc On demand Distance Vector routing (AODV) protocol the routes are found only on need and the connection setup delay is less. An authenticated secure data communication protocol E-AODV (Energy based AODV) is proposed in this work which ensures the security of Confidentiality, Integrity and Availability triangle. Confidentiality is provided by calculating Intermediate Trust Value (ITV) for all nodes between source and destination and only the nodes which possess highest ITV is used for data transmission. Integrity is attained by an encryption algorithm called digital signature algorithm which is used at the time of data transmission from source to destination node. Availability have been provided by calculating the residual energy of each node so that nodes which possess highest energy are used for data transmission. Simulation results using NS2 also prove that the performance level of throughput, Energy consumption and packet delivery ratio in E-AODV increases with that of AODV routing protocol. The results obtained are trained using Back propagation algorithm and the effectiveness of the proposed system is checked by ANN approach.

Keywords: Availability, Confidentiality, Digital Signatures, Energy, Integrity, Trust

1. Introduction

CIA triangle can be defined as the industry standard for computer security based on three characteristics of information such as Confidentiality, Integrity and Availability[1]. These three important characteristics in CIA triangle are shown in Figure 1. A routing protocol of MANET has its importance in handling entire network for communication and determining the routing paths.

The network contains a collection of nodes which further transfers information is in the form of packets. A good routing protocol should successfully transfer the data packets to the desired destination node[2].

Hence for preventing attacks from malicious nodes and for making a secure data communication the features to be considered are[3,4].

Figure 1. CIA Triangle.

- Confidentiality – Information is protected between authorized users.
- Data Integrity – No Unauthorized modification of original messages.
- Availability - It enables authorized users to access information without interference and receives it in the required format.

* Author for correspondence

- End to End Non-repudiation – Ensuring both the sender and the receiver are verified during data transmission.
- End to End Authentication - To ensure both the sender and the receiver are authenticated.

1.1 Problem Definition

Due to the mobility of mobile adhoc networks the scope of packet loss increases in the network. Then at the network layer, due to nodes mobility, the performance of a routing protocol degrades which decreases the throughput and packet delivery ratio. Hence networking issues such as neighbour discovery, network connectivity, scalability and routing becomes a difficult task in a MANET network.

To overcome this, Energy based AODV (E-AODV) is proposed in which a trust based energy model is considered for designing the network and residual energy is calculated for each node. The source and destination nodes selected possess peak energy level compared to other nodes. Based on the maximum intermediate trust value, residual energy level for an individual node and minimum hop distance to the destination node the forwarding nodes are selected. The packets which are to be transmitted are encrypted using digital signature algorithm which ensures a CIA Triangle based secure communication and it is described in the further sections.

2. Artificial Neutral Network Approach

2.1 Backpropagation Algorithm with Gradient Descent Based Learning

Here the basic diagram of backpropagation algorithm with input, output and hidden layers are described in Figure 2.

The simple algorithm is given as[5,6]

Weights are initialized

Repeat

Train each pattern

End

Until error is minimum.

3. Related Works

S. Umang, B.V.R. Reddy, M. N. Hoda[7] proposes a concept to detect malicious node. Whenever a node receives a packet, the sequence number status and a check for duplicate packets are done. When the node is non-malicious, then the sequence number is equal. Here impersonation of sequence number for a malicious node can be done and further message integrity of a packet transmission is not discussed.

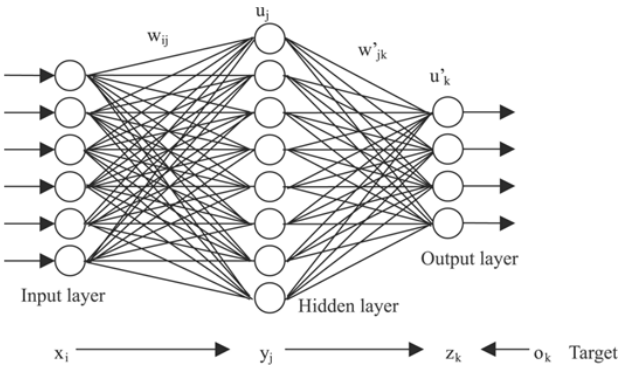

Figure 2. Basic Diagram of Backpropagation with Gradient Descent based Learning.

Preeti Bathla, Bhawna Gupta[8] proposes a methodology in which all nodes initially attains a onetime public and private key pair and a public key from the certificate authority. When the destination node receives an RREQ from source, upon verification generates a session key. Then RREP is sent from the destination along with the encrypted session key. Here the intermediate node selection is not discussed and a malicious node may also behave as an intermediate node which is not traceable.

Imran Raza, S. A. Hussain[9] proposes a guard node concept in which the behavior of guard node is detected. Since every node is a guard node, the behavior increases or decreases depending upon the neighbor nodes trust level. A node with higher trust level is considered as non-malicious and considered for route selection.

Ajay Mahimkar, R. K. Shyamsundar[10] proposes S-MECRA (Secure and Energy Efficient Routing Protocol) which ensures nodes with higher reputation number and higher residual battery capacities are only selected for data transmission. Here authentication of nodes in the network and message integrity is not discussed.

R. S, Mangrulkar, Dr. Mohammad Atique[11] implements a routing algorithm TBAODV (Trust based AODV) containing a trust factor which depends on neighbor nodes during data transmission. For detecting malicious nodes, no specific mechanism has been followed.

Seung Yi, Prasad Naldurg, Robin Kravets[12] proposes

in SAR (Security Aware Adhoc Routing) protocol that the intermediate nodes incorporates trust levels as a security metric which is embedded with the RREQ packet.

Luo and Lu[13] proposes an authentication method in which the neighbor nodes monitor the behavior of other nodes. Then the set of neighbor nodes generate a public key certificate for each node.

Various protocols with different solutions have been discussed for improving manet security[14–21].

Moradi. Z, Teshnehlab. M and Rahmani A .M.[22] proposes an ANN approach which effectively proves the DOS attack using an intruder node.

Min-Hua Shao, Ji-Bin Lin, Yi-Ping Lee[23] implements a backpropagation network and clustering technique for intrusion detection using AODV in Adhoc networks.

S. S. Manvi, M. S. Kakkasageri, S. Akhilan and S. R. Balasundaram[24] proposes a backpropagation algorithm which detects the misuse attacks in manets. Foe detecting the attacks the nodes are trained with patterns using ANN.

4. Proposed Methodology of Ensuring CIA Triangle

Proposed methodology of ensuring CIA triangle the proposed CIA triangle methodology is explained in Figure 3. The principal of the protocol E-AODV is that, the forwarding nodes used in transmission should be of high trust value and maximum energy level which avoids packet loss and the packet which is transmitted through nodes is encrypted using digital signature algorithm in MANETS which guarantees the integrity and ensures the CIA Triangle security. The further chapters explain in detail about the CIA triangle security.

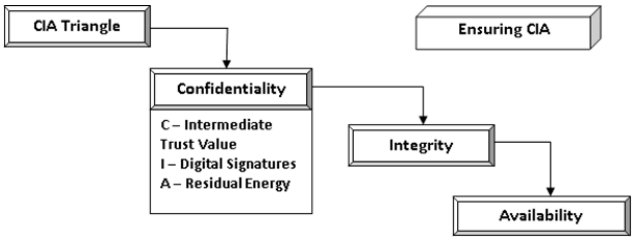

Figure 3. Proposed CIA triangle.

4.1 Ensuring Confidentiality in CIA Triangle

Confidentiality can be assured by evaluating intermediate trust values between nodes. The characteristics of intermediate trust value and evaluating procedure is discussed below.

The characteristics of trust can be given as follows[25]

- Trust is subjective.
- Trust is not transitive. (i.e.) X trusts Y and Y trusts Z but it does not imply that X trust Z.
- Trust is dynamic not static.

Since it is dynamic, for making a decision upon each node, an ITV computation for each node is a must. The following equations describe how an ITV value is calculated and used with the AODV routing protocol in MANETS. The evaluation of Intermediate Trust Value is discussed below[26].

Now in the proposed E-AODV, assume that the query request success rate of a node i which is shown in equation 5 as

$$q_r s(i) = a \tag{5}$$

The query response failure of a node i can be given in equation 6 as

$$q_r f(i) = b \tag{6}$$

Hence the query request for node i is calculated in equation 7 as

$$q_r(i) = \sum \frac{q_r s_i - q_r f_i}{q_r s_i + q_r f} \tag{7}$$

Here assume that the request for a node which is given in equation 8 as

$$r_q = 0.1 \tag{8}$$

Similarly the response for a node in equation 9 as

$$r_p = 0.1 \tag{9}$$

and K = 1000 (i.e) maximum rate of packets to be transmitted in Kbytes.

Now the data query request success of a node i can be given in equation 10 as,

$$dq_r s_i = c \tag{10}$$

Similarly the data query response failure of a node i can be given in equation 11 as,

$$dq_r f(i) = d \tag{11}$$

The data query request for node i can be given in equation 12 as,

$$dqr(i) = \sum \frac{dq_r s(i) - dq_r f(i)}{dq_r s(i) + dq_r f(i)} \tag{12}$$

Now the intermediate trust value can be calculated in equation 13 as

$$ITV(i) = \frac{\sum [r_q * q_r(i)] + [r_p * dq_r(i)]}{k} \tag{13}$$

4.2 Ensuring Availability in CIA Triangle

For ensuring availability in CIA triangle, consumed energy is calculated for each node and residual energy for each node is found out which is discussed below.

POWER CONSUMPTION

An insufficient energy node cannot be able to participate in data transmission[27].

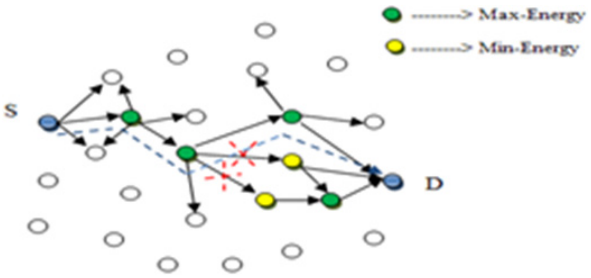

Figure 4. Routing Scheme with Energy Selection.

The routing nodes with maximum and minimum energy selection is shown in Figure 4. Every node checks the energy periodically for power consumption. Each node transmits energy by sending or receiving data packets[28,29]. Initially consider all nodes energy level as 100%. The remaining energy is calculated as follows.

Energy used for single packet transmission is given in equation 14 as

$$\text{Used Energy} = P_t * T \quad (14)$$

P_t - transmitting power and T – time taken for transmission.

Energy used for single packet receiving is given in equation 15 as

$$\text{Used Energy} = Pr * T \quad (15)$$

P_r - receiving power and T – time taken for transmission. The value T is given in equation 16 as

$$T = \text{Size of the packet} / \text{Packet Rate} \quad (16)$$

Hence the residual energy can be calculated as shown in equation 17.

$$Energy_{res} = \text{Current Energy} - \text{Consumed Energy} \quad (17)$$

Using the calculated ITV values and residual energy of each node a decision has to be made for node selection for transmitting data[30]. When nodes are selected using this decision box, it ensures confidentiality and availability of a node in CIA triangle security. When residual energy is high, it is considered that the node is available throughout the data transmission and it cannot be a selfish (or) malicious node.

4.3 Ensuring Integrity in CIA Triangle

Integrity can be assured in the proposed methodology using digital signatures which is discussed below.

Table 1. Decision making using ITV and residual energy for node selection

S.NO	ITV of a node	Residual Energy in %	Decision Making for node selection
1	≥ 0.7	> 80	Extremely higher Priority
2	≥ 0.7	60 - 80	Very High Priority
3	≥ 0.5 & < 0.7	> 80	High Priority
4	≥ 0.5 & < 0.7	60 - 80	Medium Priority
5	< 0.5	50 - 100	Low Priority
6	< 0.5	< 50	Very Low & Rejected List

A digital signature is an authentication tool which can be formed by encrypting the original message with sender's private key[31]. Further for attaining confidentiality, the original message with signature is further encrypted with the receiver's public key. Hence data integrity can be guaranteed for a given message when using digital signatures. The decision making for node selection in the proposed methodology is shown in Table 1.

5. Processing Of E- AODV Protocol

Table 2. Notations used

S.No	Notations	Meaning
1	RIT	Routing Information Table
2	Sid	Source ID
3.	Did	Destination ID
4	Bid	Broadcast ID
5	Rid	Reply ID
6	Rreq	Route Request
7	Rrep	Route Reply
8	Rerr	Route Error
9	AP	Authentication Path
10	H(M)	Hashed Message
11	H(Sid(M))	Hashed Message calculated by Source ID
12	H(Did(M))	Hashed Message calculated by Destination ID
13	Sku	Source Public Key
14	Sign(Skr)	Source Private Key
15	Dku	Destination Public key
16	SignDkr	Destination Private Key
17	Eid	Error ID
18	Seq no	Sequence Number

The E-AODV setup phase consists of

- Initialization Phase
- Authentication Phase
- Data Transmission Phase
- Result Phase

The notations used in the following phases are listed in Table 2.

5.1 Initialization Phase

- All the nodes are initialized in MANETS by each node having its own IP address, MAC address and sequence number.
- Further each node is enhanced with a pair of public key and private key using public key cryptosystem by self-generation.
- After initialization is done with the node's IP, MAC address and key updation, the nodes send signal to find the number of other nodes within range.
- The synchronization between nodes takes place and the neigbour's list for each node is maintained in the RIT.
- The source and destination nodes are selected which have peak energy when compared with other nodes in the network.
- For trust calculation ITV is calculated for each intermediate node between source and destination.
- Residual energy for each node is calculated at the time of data transmission. Initially it is assumed to have 100% of energy.
- Using the decision making method as shown in Table 1, the node selection for data transmission is selected based on ITV and residual energy value which ensures confidentiality and availability.

Now each node has its own sequence number, IP address, MAC address, public key and private key as its unique ID. Further each node maintains its own neighbour's list with ITV and residual energy value for communicating packets. So before data packet transmission starts between the nodes, the nodes are initialized with these parameters. (i.e.) Except private key all other IP, MAC addresses and public key are known to all other nodes within the network initially.

5.2 Authentication Phase

AODV is a well known reactive protocol. Various process involved in this phase are described below.

5.2.1 Route Request Process

According to our protocol E-AODV, the Rreq source node packet carries the

Source ID (Source Seq no, IP address, MAC address, Public Key), Destination ID (Destination Seq no, IP address, MAC address, Public Key), Bid, AP ( )).

AP stands for Authentication Path which is initially empty when Rreq packet is broadcasted. Initially the source node floods the Rreq packet to its neighbour's list which is maintained in the RIT. Suppose if the same Rreq packet is received multiple times for the same node, which can be identified by its unique Sid, Did and Bid, the duplicate packets are discarded. The Bid is incremented each time for another Rreq packet. According to the AODV protocol the receiving neigbour nodes send back ready signals if it has the shortest route available to the destination.

5.2.2 Route Reply Process

The Rrep packet can be send by an intermediate node as

Source Seq.No, Destination Seq.No, Intermediate Node ID (Intermediate node Seq. No, ITV, IP Address, MAC Address, Public Key, Energy Value, Rid)

Here our secure protocol E-AODV is implemented such that within the ready signal neighbour nodes, the authenticated nodes must be selected. This is the challenging problem faced today in the security issues of MANETS, of these neighbour nodes which send ready signal, the nodes which have maximum ITV, residual energy and shortest hop distance to the destination is considered and further the selected nodes are considered as a secured node and are added in the Authentication Path. This node selection process continues until it reaches the destination. Each time when we find a secured node, it will be updated in the AP which is found in the Rreq packet and is maintained by the source node. Now we have found a security enabled authenticated path till the destination. Now the data transmission starts with the digital signature algorithm which hashes the data packet to be sent.

5.2.3 C Data Transmission Phase

A hash function is an authentication mechanism which changes a lengthy message to a fixed length hash value.

Now the data packet which is to be sent is hashed and the packet becomes a hashed message H (m)[32]. Now the source node calculates the hash value of the message and is stored as H (Sid (M))[33].

H (M) ====> H (Sid (M))

Then the hashed packet is digitally signed using the sender's (source) private key first which provides authentication and data origin confidentiality from the source[34].

H (M) ====> E (SignSkr H (M))

(SignSkr H (M)) ====> α

Then again the source signed hashed message is encrypted using the receiver's (destination) public key as a second signature[34,35]

(SignSkr H (M)) ====> E (Dku (SignSkr H (M)))

(Dku (SignSkr H (M))) ====> β

Then these double signed data packet β is transmitted from the source to the destination as per the order maintained in the AP which is stored in the route request packet. When the data transmission completes till the destination, then all the AP data will be erased. Suppose if another data packet transmission has to be sent from the same source and destination nodes then a new route request has to be initiated from the source and a new AP will be selected from the source to destination for security purposes.

Suppose if a link breakage occurs between the intermediate authenticated nodes (or) any packet drop occurs in the intermediate nodes at the time of transmitting packets due to energy loss then a route error message will be invoked from that node and the node will be immediately removed from the AP as well as in the RIT as an authenticated node. Here it is assumed that a packet drop occur when a node becomes a malicious or a selfish node. So for avoiding such misbehaving nodes it is removed from the AP and RIT at the time of transmission.

5.2.4 Route Error Process

The Route error message can be given as

Rerr (Error Intermediate Node ID (Seq. No, IP Address, MAC Address, Public Key, Eid)

Then the next nearest neighbour with authentication is selected from the RIT and updated in the AP. Finally the data packet reaches the destination through the secured nodes successfully and a secure data communication is possible through the E-AODV protocol.

5.2.5 D Result Phase

After the destination node is reached, the receiver has to decrypt the double signed data packet.

(Dku (SignSkr H (M))) ====> β

D (SignDkr (β) ====> (SignSkr H (M))

(SignSkr H (M)) ====> α

D (Sku (α)) ====> H (M)

H (M) ====> H (Did (M))

First the receiver (destination node) decrypts using the receiver's private key. Further the hashed data packet is again decrypted using the sender's public key to which ensures confidentiality, authentication and non-repudiation of source and destination[36]. At last the hashed data packet is recomputed to find the original data packet and to ensure data integrity.

H (Did (M)) ====> H (Sid (M))

6. Simulation Set Up

For simulation of proposed protocol, NS-2 simulator tool has been used. Both AODV and E-AODV protocols in network simulator 2.34 version have been simulated and the performance results are compared between the protocols[37]. Here we select 50 nodes which are arranged in a MANET topology of network area 2000x2000 meters. Using the nam simulator trace files the various parameters such as throughput, packet delivery ratio, delay, node density and security performance are analyzed. The various parameters used are listed in Table 3.

Table 3. Parameters Used

Parameters	Assumptions
Simulator Tool	NS-2 (version 2.34)
No. of nodes	50
Minimum delay required	2 CBR units
Maximum delay required	7 CBR units
Minimum bandwidth required	4 CBR units
Network Area	2000x2000 meters
Transmission range	250 meters
MAC layer protocol	IEEE 802.11
Protocol	AODV,E-AODV
No. of packets	1000

6.1 Node Density Comparison

Here the performance of packet delivery ratio is measured with the increase in node density. The AODV packet delivery ratio reaches a maximum threshold at node density 20 and then decreases when the number

of nodes increases since the packet drop is more in normal AODV which is shown in Figure 5. But E-AODV attains a high packet delivery ratio even though the node increases because the selected nodes for transmission are of high ITV with maximum energy and of its security enhancement during transmission which avoids packet loss.

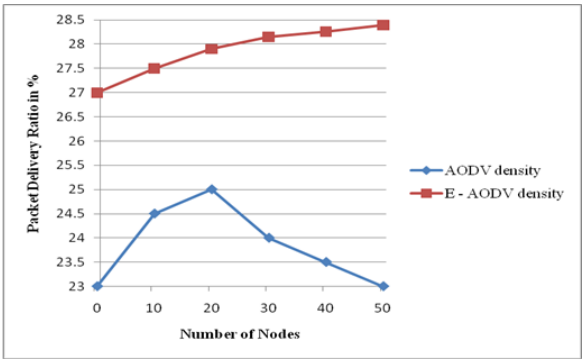

Figure 5. Comparision of Density.

6.2 Delay Comparison

The delay can be said as the time taken for a packet to travel from source to the destination and also includes route discovery, authentication enhancement transfer time. In Figure 6, the two protocols used are compared at various pause time intervals. E-AODV has slightly higher delay due to strong authentication and reliability and selecting energized nodes for transmission.

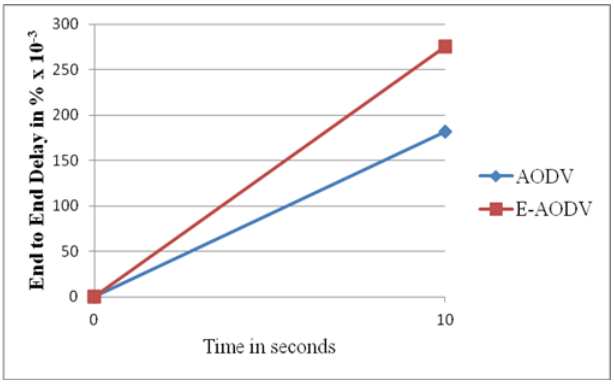

Figure 6. Comparision of Delay.

6.3 Packet Delivery Ratio Comparison

Comparison of packet delivery ratio is shown in Figure 7. The AODV attains a maximum threshold PDR at pause time 4 and maintains a constant PDR. When compared to AODV, E-AODV performance PDR increases with time since the network life time of a node is increased using the trust, energy model and security enhanced because of the digital signature algorithm used in the network which ensures less packet loss occurrence during transmission.

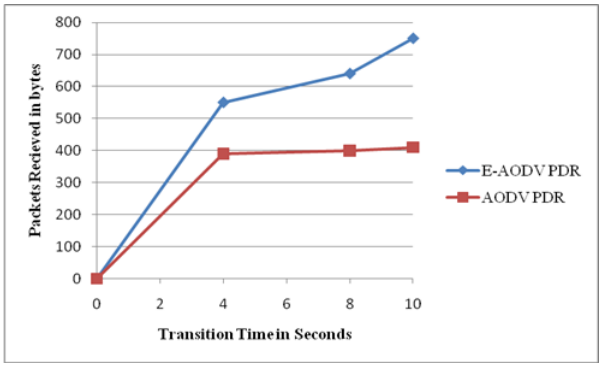

Figure 7. Comparision of Packet Delivery Ratio (PDR).

6.4 Throughput Comparison

The comparison of throughput is shown in Figure 8. When compared to AODV, E-AODV gives a constant high throughput since it encrypts the packet which provides authentication and security. Further the nodes high ITV with maximum energy and minimum hop distance to the destination are selected for transmission which ensures high throughput value.

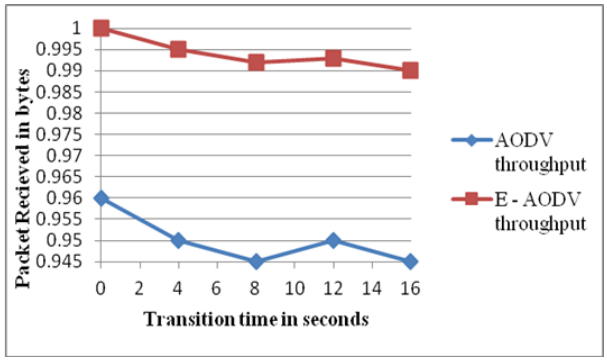

Figure 8. Comparision of Throughput.

6.5 Energy Consumption Comparison

The energy consumption graphs are compared for the two protocols AODV and E-AODV. When AODV is used for transmission, it does not check for any energy value for the nodes used in transmission which makes packet loss and the energy also decreases. But in case of E-AODV

residual energy is calculated which ensures nodes having maximun energy only is used for transmission which makes the energy level maintain in the same level and the increase in the network lifetime of an individual node which is shown in figure 9. From the simulation results it is found that the performance level of E-AODV is more than normal AODV routing protocol.

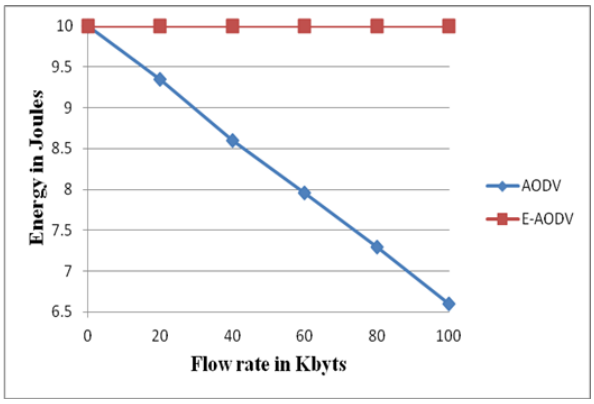

Figure 9. Comparision of Energy Consumption.

7. Backpropagation Algorithm with Gradient Descent based Learning Implementation

The various training parameters of gradient descent based learning with their assumptions and results are discussed in Table 4.

Table 4. Gradient Descent based Learning Training Parameters

S.NO	Parameters	Assumptions and Results
1	The number of neuron on the layer	Input:2,Hidden:4,Output:1
2	Training Parameter Learning Rule	Backpropagation
3	Mean Squared Error	0.000991445
4	Best Training Performance	514 Epochs
5	Gradient	1.15320
6	Training Rate	0.05
7	Validation Check	0.001 at epoch 514

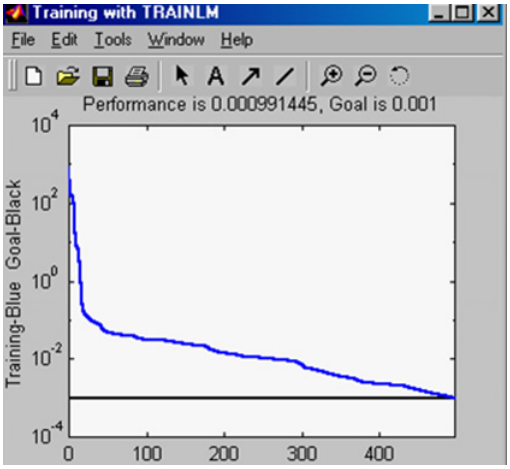

Figure 10. Epoch Diagram using ANN.

Table 5. Comparison of Throughput of Actual Values with Predicted Values

S.NO	Transition Time(sec)	AODV Throughput	E-AODV Throughput (Actual Output)	Predicted Output	Error Value
1	0	0.96	1	0.55	0.45
2	2	0.955	0.998	1.118	-0.12
3	4	0.95	0.995	0.315	0.68
4	6	0.948	0.994	0.674	0.32
5	8	0.945	0.992	1.832	-0.84
6	10	0.947	0.993	0.853	0.14
7	12	0.95	0.995	0.555	0.44
8	14	0.949	0.992	1.582	-0.59
9	16	0.945	0.99	0.8	0.19

In this study, prediction of throughput of E-AODV was studied by using a backpropagation neural network that uses gradient descent based learning algorithm. Comparison of results have been done for both simulation and ANN. Transition time in seconds and AODV throughput are given as input and throughput of E-AODV is recorded as output parameters. Comparison of simulated E-AODV throughput results with the predicted output is shown in table 5. Finally error value is calculated for each transition time.

From Table 5 similar results have been attained between trained data values and simulated values. The training performance reaches the goal 0.001 at epoch value 514. Hence attaining the goal 0.001 with mean squared error value of 0.000991445 at epoch value 514 is shown in Figure 10. These training methods have been similar to the works carried by [22] and [24].

8. Conclusion

Hence the proposed Energy based secure protocol E-AODV (Energy based AODV) which secures data using digital signature algorithm enhances the throughput and security. E-AODV attains a high throughput even though the node increases because of its Trust and Energy model used and security enhancement which is shown in the simulation results. Further increase in packet delivery ratio with time concludes that our proposed E-AODV not only provides authenticated path in MANETS but also assures confidentiality, data integrity, availability, end to end authentication and end to end non-repudiation during packet transmission in networks. Finally it is assured that using backpropagation algorithm with gradient descent based learning ensures CIA triangle in the proposed E-AODV protocol. Simulation results using NS2 also prove that the performance level of throughput, Energy consumption and packet delivery ratio in E-AODV increases with that of AODV routing protocol. Finally the original results obtained are trained using Backpropagation algorithm. An ANN approach is used to check the effectiveness of the proposed system and is analyzed in terms of mean square error value, learning rate, gradient value and finally the backpropagation network also ensures CIA Triangle security in E-AODV.

9. References

1. Whitman ME, Mattord HJ. Principles of Information Security. India: Vikas Publishing House; 2003.
2. Siva Ram Murthy C, Manoj BS. Wireless Networks Architectures and Protocols. 1st edn. India: Pearson Education; 2004.
3. Mishra A, Nadkarni KM. Security in wireless adhoc networks in: The handbook of wireless Adhoc networks. CRC press M. Ilyas edn. 2003.
4. Stallings W. Cryptography and network security- principles and practices. 3rd edn. India: Prentice Hall; 2005.
5. Rajasekaran S, Vijayalakshmi Pai GA. Neural networks, fuzzy logic, and genetic algorithms synthesis and applications. Prentice Hall of India, 2003.
6. Kumar S. Neural networks – A classroom approach. 1st ed. New Delhi: Tata McGraw Hill; 2005.
7. Umang S, Reddy BVR, Hoda MN. Enhanced intrusion detection system for malicious node detection in adhoc routing protocols using minimal energy consumption. IET Communications. 2010 Nov; 4(17):2084–94.
8. Bathla P, Gupta B. Security Enhancements in AODV Routing Protocol. International Journal of Computer Science and Technology. 2011 Jun; 2(2):295–8.
9. Raza I, Hussain SA. Identification of Malicious nodes an AODV pure Adhoc network through guard nodes. Computer Communications. 2008 Jun; 31(9):1796–802.
10. Mahimkar A, Shyamsundar RK. S-MECRA: A secure energy efficient routing protocol for wireless Adhoc network. IEEE 60th Vehicular Technology Conference, India. 2004. p. 2739–43.
11. Mangrulkar RS, Atique M. Trust based secured Adhoc on demand distance vector routing protocol for mobile Adhoc network. Proceedings of 6th International Conference on Wireless Communication and Sensor Networks; IEEE. 2011. p. 1–4.
12. Yi S, Naldurg P, Kravets R. Security aware Adhoc routing for wireless networks MobiHoc '01. Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking and computing, New York, USA: ACM; 2001.
13. Luo H, Lu S. Ubiquitous and robust authentication services for Adhoc wireless networks. UCLA-CSD-TR-200030.
14. Moamen AA, Hamza HS, Saroit IA. Secure multicast routing protocols in mobile ad-hoc networks. International Journal of Communication Systems. 2013 Jan; 31:2508.
15. Rajesh Babu M, Selvan S. A light weight and attack resistant authenticated routing protocol for mobile Adhoc networks. International Journal of Wireless and Mobile Networks. 2010 May; 2(2):16–29.
16. Wang C-F, Ding J-W, Chen T-C. A routing protocol for mobile adhoc networks using the profit optimization model. International Journal of Communication Systems. 2013 Feb. Available from: 10.1002/dac.2511.
17. Singh K, Yadav RS, Ranvijay. A review paper on Adhoc network security. International Journal of Computer Science and Security. 2007 Jul; 1(1):52–69.
18. Kostin A, Oz G, Haci H. Performance study of a wireless mobile ad hoc network with orientation dependent internode communication scheme. International Journal of Communication Systems. 2012 May. Available from: 10.1002/ dac.2363.
19. Sreepathi S, Venigalla V, Lal A. A survey paper on security issues pertaining to Adhoc networks. Information Systems Security. CSC 574.
20. Jaafar MA, Zukarnain ZA. Performance comparisons of AODV, secure AODV and adaptive secure AODV routing protocols in free attack simulation environment. European Journal of Scientific Research. 2009; 32(3):430–43.

21. Patwardhan A, Parker J, Iorga M, Karygiannis T, Yesha Y. Threshold based intrusion detection in adhoc networks and secure AODV. Adhoc Networks, Elsevier; 2008; 6:578–99.
22. Moradi Z, Teshnehlab M, Rahmani AM. Implementation of neural networks for intrusion detection in manet. International Conference on Emerging Trends in Electrical and Computer Technology. India. 2011. p. 1102–6.
23. Shao M-H, Lin J-B, Lee Y-P. Cluster based cooperative back propagation network approach for intrusion detection in MANET. 10th International Conference on Computer and Information Technology. IEEE; 2010 Jul.
24. Manvi SS, Kakkasageri MS, Akhilan S, Balasundaram SR. Artificial neural network based misuse detection in MANETs. IJCA Journal In : International Conference on VLSI, Communications and Instrumentation. 2011; 2(1).
25. Seshadri Ramana K, Chari AA, Kasiviswanth N. Review and analysis of trust based routing in manets. International Journal of Computer Science and Research. 2010; 1(1):50–68.
26. Sumathi A, Vinayagasundaram B. Evaluating an authenticated trust based adhoc on demand distance vector for malicious node isolation in manets. Journal of Computer Science. 2014; 10(9):1859–64.
27. Dhurandher SK, Misra S, Obaidat MS, Bansal V, Singh PR, Punia V. EEAODR: An energy-efficient adhoc on demand routing protocol for mobile adhoc networks. International Journal of Communication Systems. 2009 Jul; 22(7):789–817.
28. Laura. Energy Consumption model for performance Analysis of routing protocols in MANET. Journal of Mobile Networks and Application. 2000.
29. Li X, Miao J-S. A new traffic allocation algorithm in Adhoc networks. The Journal of China University of Post and Telecommunications. 2006 Sep; 13(3).
30. Pushpalatha M, Venkataraman R, Ramarao T. Trust based energy aware reliable reactive protocol in mobile ad hoc networks. World Academy of Science, Engineering and Technology. 2009; 56:16–9.
31. Rivest RL, Shamir A, Adelman LM. A method for obtaining Digital Signatures and Public Key Cryptosystems. Commun, ACM. 1978; 21(2):120–6.
32. Lamport L. Constructing Digital Signatures from a one way function. Technical report SRI International, CLS 98, 1979 Oct.
33. Merkle R. A digital signature based on a conventional encryption function. CRYPTO'87, LNCS. 1987; 293:369–78.
34. Micali S, Rivest R. Transitive Signature Schemes. Topics in Cryptology – CT-RSA 2002, Springer-Verlag; 2002. p. 236–43.
35. Reyzin L, Reyzin N. Better than BIBA: Short one- time signatures with fast signing and verifying. Proceedings of 7th Australasian Conference on Information Security and Privacy; LNCS 2384. 2002 Apr.
36. Xu S, Mu Y, Susilo W. Secure AODV routing protocol using one time signature. Proceedings of 1st International Conference on Mobile Ad-hoc and Sensor Networks MSN 2005, Springer; LNCS 3794. 2005 Dec.
37. Hou T-C, Chan M-C, Wu C-M. Analysis of MANET dynamic source routing and its performance enhancements. International Journal of Communication Systems. 2013. Available from: 10.1002/dac.2512.