Engineering and Scientific International Journal (ESIJ)
Volume 1, Issue 1, October - December 2014
ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

SE-AODV-Secured and Energy Efficient Routing in Mobile Ad-hoc Network

S.Sridhar[#1], R.Baskaran[*2]

[1]*Department of Computer Applications, S. A. Engineering College, Chennai – 77, India*
ssridharmca@yahoo.co.in
[2]*Department of Computer Science & Engineering, CEG, Guindy, Anna University, Chennai-25, India.*
baskaran.ramachandran@gmail.com

Abstract— Mobile ad hoc network (MANET) is a standalone network capable of autonomous operation where nodes communicate with each other without the need of any existing infrastructure. Mobile ad hoc networks consist of nodes that cooperate to provide connectivity and are free to move and organize randomly. Every node is router or an end host, in general autonomous and should be capable of routing traffic as destination nodes sometimes might be out of range. Nodes are mobile since topology is very dynamic and they have limited energy and computing resources. These nodes are often vulnerable to failure thus making mobile ad hoc networks open to threats and attacks. Communication in MANET relies on mutual trust between the participating nodes but the features of MANET make this hard. Nodes sometimes fail to transmit and start dropping packets during the transmission. Such nodes are responsible for untrustworthy routing. Nodes should also be considered for sufficient energy levels to make transmission. A secured scheme can be used to track these untrustworthy nodes and isolate them from routing, thus provide trustworthiness. In this paper a secured and energy based AODV (SE-AODV) protocol is presented which implements a message digest algorithm for every transmission. Energy is introduced and nodes are considered for routing only if they have energy level higher than the threshold (Average energy value of nodes considered for routing). The SE-AODV increases PDR and decreases delay thereby enhancing the QoS metrics and trustworthiness in AODV based MANET routing. The work is implemented and simulated on NS-2. The simulation result shows the proposed SE-AODV provides more trustworthy routing compared with general AODV.

Keywords— *Ad-hoc, MANET, AODV, SE-AODV, Trust, Qos*

1. Introduction

A Mobile ad hoc network is an enormously difficult dynamic network. Mobile Ad-Hoc network [1] is a system of wireless mobile nodes that self-organizes itself in dynamic and temporary network topologies. Nodes can connect and depart the network at anytime and should be in position to relay traffic. The primary goal of MANET is to find an end to end path or route, minimizing overhead, loop free and route maintenance. A few challenges faced in mobile ad hoc networks are mobility, variable link quality, energy constrained nodes, heterogeneity and flat addressing.

Most traditional mobile ad hoc network routing protocols were designed focusing on the efficiency and performance of the network [2]. These protocols should meet some basic requirements like self starting, self organizing, loop free paths, dynamic topology maintenance, minimal traffic overhead etc to deal with the challenges involved in routing. Existing MANET routing protocols can be classified into mainly two types- proactive routing protocols and reactive routing protocols. Table driven (proactive) routing protocols such as dynamic Optimized Link State Routing (OLSR), Destination-Sequenced Distance-Vector routing (DSDV), Topology Broadcast based on Reverse Path Forwarding (TBRPF) and On-demand (reactive) routing protocols such as Ad hoc On demand Distance Vector (AODV), Signal Stability-based Adaptive routing (SSA), Dynamic Source Routing (DSR). Other categories are flooding based, cluster based, geographic and application specific. Proactive protocols are table driven protocols much similar to conventional routing, have little delay in route discovery and routing overhead is high. On-demand routing protocols are reactive protocols which obtain route information only when needed and the overhead is low since there is no periodic update of tables.

AODV is a reactive protocol where route discovery initiated when required only using route request (RREQ) and route reply (RREP) packets and stores only active routes in routing table. Explicit route error notification is done by using route error (RERR). Ad-hoc on demand Distance Vector (AODV) routing protocol [3] is an on demand routing protocol that focuses on discovering the shortest path between two nodes with no consideration of the reliability of a node. By broadcasting HELLO packets in a regular interval, local connectivity information is maintained by each node. However, the traditional AODV protocol seems less than satisfactory in terms of delivery reliability there by affecting quality of service.

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

Due to the dynamic nature of Mobile Ad-Hoc Networks, there are many issues which need to be tackled and one of the areas for improvement is Quality of Service (QoS) routing. When it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met [4]. A few challenges faced in providing Qos are persistently changing environment, unrestricted mobility which causes recurrent path breaks and also make the link-specific and state-specific information in the nodes to be inaccurate.

This SE-AODV protocol calculates energy values for every node that takes part in routing and compares it with threshold value calculated based on average energy value of all nodes. Thus node with sufficient energy is considered for routing and all transmission done are secured using message digest algorithm. This scheme facilitates in providing secured and energy efficient routing in MANET and also improves the performance Qos parameters like PDR and delay.

2. Literature Survey

Mobile ad hoc network is capable of autonomous operation, operates without base station infrastructure, nodes cooperate to provide connectivity and operate without centralized administration. MANETs have put on more significance in recent applications areas like security, routing, resource management, quality of service etc. The significance of routing protocols in MANETs has anticipated for a lot of competent and inventive routing protocols. Continuous evaluation of node's performance and collection of neighbour node's opinion value about the node are used to calculate the trust relationship of this node with other nodes [5]. In this paper, existing AODV routing protocol has been modified in order to adapt the trust based communication feature and the proposed trust based routing protocol equally concentrates both in node trust and route trust.

RAODV (Reliant Ad hoc On demand Distance Vector Routing) [6] is a security-enhanced AODV routing protocol that uses a modified scheme called direct and recommendations trust model and then incorporating it inside AODV. This scheme assures that packets are not handed over to malicious nodes. Based on this trust value a node is selected to perform packet transfer. This protocol results in higher percentage of successful data delivery compared to AODV. A routing algorithm is proposed that adds a field in request packet which stores trust value indicating node trust on neighbor [7]. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all that results not only in saving the node's power but also in terms of bandwidth. A trusted path irrespective of shortest or longest path is used communication in the network.

A routing protocol [8], that adds a field in request packet and also stores trust value indicating node trust on neighbour based on level of trust factor. This scheme avoids unnecessary transmit of control information thus efficiently utilizing channels and also saves nodes power. Route trust value is calculated based on the complete reply path, which can be utilized by source node for next forthcoming communication in the network that results in improvement in security level and also malicious node attacks are prevented. A trust based packet forwarding scheme [9] for detecting and isolating the malicious nodes using the routing layer information that uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node will be punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.

A framework [10] for estimating the trust between nodes in an ad hoc network based on quality of service parameters is proposed based on Probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays. It has been shown that only two end nodes need to be involved and thereby achieve reduced overhead. A Node-based Trust Management (NTM) scheme in MANET [11] is introduced based on the assumption that individual nodes are themselves responsible for their own trust level. Mathematical framework of trust in NTM is developed along with some new algorithms for trust formation in MANETs based on experience characteristics offered by nodes. The above listed works are spotlighting on reliability that is provided to the mobile ad hoc network by using trust schemes.

3. Proposed Work

In MANET, providing reliable routing is difficult because of its dynamic nature that keeps nodes moving and not stable. In spite of this nature, nodes communicate with each other and exchange data among the nodes that are in its range on the network. But still there are nodes in the MANET which take part in routing but drop packets while transmitting packets which affects the performance of the protocol. Thus SE-AODV is introduced which checks each node before involving it in the routing process. The design of the proposed work is presented in Fig. 1.

In the MANET an observation is made on all nodes that transmit packets. Energy values are introduced for every node and is calculated based on their transmission and reception power. The total packets they transmit, packets they receive and the packets they drop are taken in to account. Once a particular transmission is to be made the protocol decides the route and the nodes which are going to participate in routing are checked against their energy

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

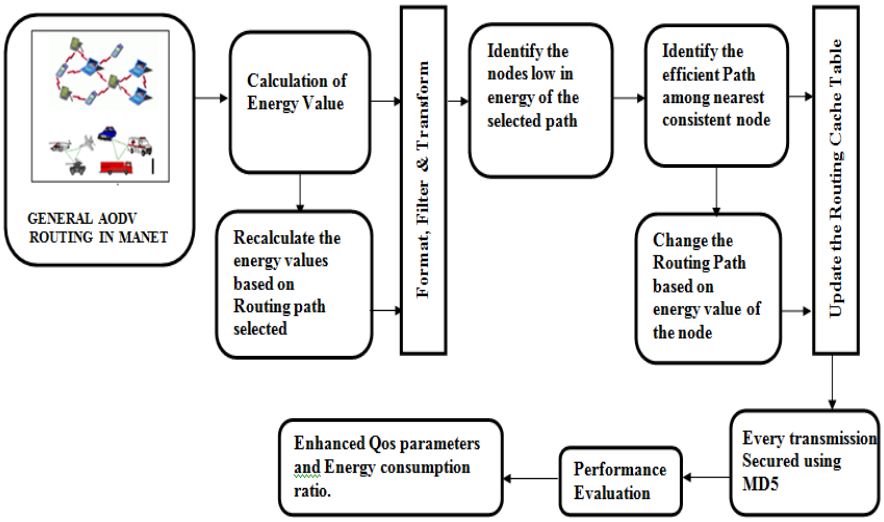

Fig.1: Architecture of SE-AODV routing in MANET

values. Based on this energy value a node is located if it is about to drop packets. Thus these packet dropping nodes are spotted and removed from the routing path and the protocol again checks for an alternate node for proceeding the routing. Thus an alternate path is identified based on the energy values of the node that is to be included recently in the routing path to carry on the routing effectively.

3.1 MD5 for Secured Transmission

The critical job in routing is to identify the attackers in the path. To identify the attackers we initially set (flag) all nodes as true nodes. Nodes change their nature only after performing transmissions. Nodes properties considered are IP Address (IP), Nodes identification (ID), MAC Address and msg. If any one of these property of a node is altered or changed, we conclude the node is an attacker. We propose that change in ip address concludes the node as attacker. Initially ip is set in a sequence. Example set ip_node0 192.26.2.0; set ip_node1 192.26.2.1; set ip_node2 192.26.2.2; set ip_node3 192.26.2.3; set ip_node4 192.26.2.4; set ip_node5 192.26.2.5

If any node uses another ip which already exists then we conclude that node as attacker. Ip address is set in sequence. For instance node 5 and node 10 has same ip address, then check node's flag whether its true or false. It would be true for node 5 but false for node 10 since the ip is replicating for node 10. Since we have set ip addresses in sequence it's clear that the current ip address of node originally belongs to node 5. These algorithms operate on a message 512 bit at a time. Pad the msg to a multiple of 512 bits. Digest calculation begins with digest value initialized to a constant. This value is combined with first 512 bits of msg to produce a new value for the digest; using a complex transformation. New value is combined with next 512 bits of msg using same transformation and so on until final value of digest is produced. The main ingredient of MD5 alg is the transformation that takes input as current value of the 128 bit digest, plus 512 bits of msg and outputs a new 128-bit digest. MD5 operates on 32 bit quantities. Current digest value can be thought of as four 32-bit words(d0, d1, d2, d3) & piece of msg currently being digested (512) as sixteen 32 bit words (M_0 through M_{15}).

First pass- New digest is produced from old value & the 16 msg words using 16 steps. Process continues until all 16 words (till M_{16}) have been digested. Second pass--same as first pass with following difference. F is replaced by a slightly diff function G. Constant T_1 through T_{16} are replaced by another set (T_{17} through T_{32}) .Amount of left rotation is {5, 9, 14, 20, 59..} at each step . Instead of taking bytes of msg in order M_0 through M_{15}, the msg byte that is used at stage i is $M_{(5i+1) \bmod 16}$. Third pass- G is replaced by function H (XOR of its arguments), another set of constants (T_{33} thru T_{48}), amount of left rotation {4, 11,16, 23, 4, 11..} at each step and msg byte used at stage I is $M_{(3i+5) \bmod 16}$. Fourth pass- H replaced by function I (combination of bitwise XOR, OR & NOT), another set of constants (T_{49} thru T_{64}), mount of left rotation {6, 10, 16, 21, 6, 10...} and msg byte used at stage is is $M_{7i \bmod 16}$.

4. Evaluation Results

The proposed SE-AODV protocol's performance is analyzed using NS-2 simulator. The network is planned and implemented using network simulator with node size varying from 25 to 300 and other parameters based on which the network is shaped are given in Table. 1. The simulator is applied with traditional AODV and with proposed SE-AODV and results are obtained for assessment. The proposed SE-AODV protocol has shown good progress over the Qos parameters like PDR & Delay.

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

PDR is increased and delay is reduced compared to the traditional AODV and throughput is maintained in both cases. However there is a fraction of difference in throughput between general and proposed protocol which is rounded off as a whole value in result table. The performance of the proposed protocol is also represented graphically where it clearly shows the betterment of the Qos parameters.

Parameter	**Value**
Network size	1600 x 1600
Number of nodes	25 – 300
Movement speed	100 kbps
Transmission range	250 meters.
Packet size	5000
Traffic type	CBR
Simulation time	30 minutes.
Maximum speed	100 kbps
MAC layer protocol	IEEE 802.11
Time interval	0.01 sec.
Protocol	AODV
NS2 version	2.34

Table1. Simulation Parameter Values

Fig. 2. shows the snapshot of the simulation which contains 50 nodes. Node 1 is the source and node 34 is the destination. The initial routing path is node 1 – node 5 – node 20 – node 28 – node34. Fig. 3. shows the snapshot where transmission goes on between source and destination while network identifies misbehaving node due to less energy level. Node 5 drops packet so identified as misbehaving node. Fig. 4. shows the routing has taken an alternate path thus avoiding misbehaving node. The new path is node 1 → node6 → node 4 →node 15→ node 20→node 29 → node 33→ node 34.

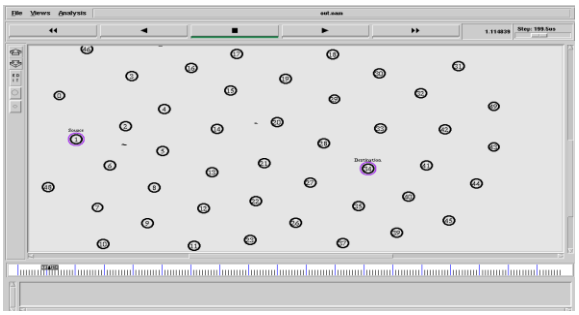

Fig.2: Snapshot showing 50 nodes in MANET

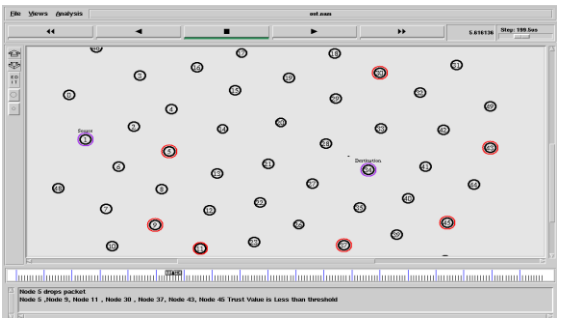

Fig. 3 Snapshot showing Misbehaving nodes

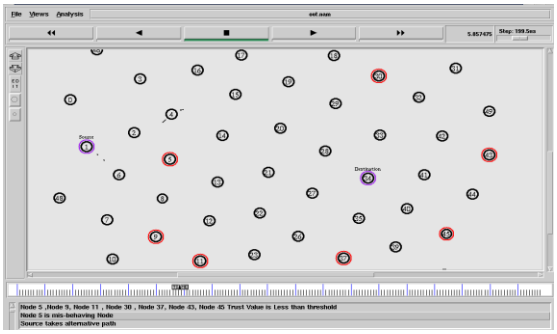

Fig. 4 Snapshot showing Routing taking alternate path

4.1 Security scheme scenarios

The nodes are marked initially as true and as transmission starts they start changing.
Flag for node(1)--------> true
Flag for node(2)--------> true
Flag for node(9)--------> flase
Flag for node(28)-------->flase

Routing Path	: N23 , N1 , N40 , N41 , N48
Mis-behaving Routing	: N23 , N9 , N28 , N48
Alternative Routing	: N23, N1,N2, N40, N41,N48

Mis-behaving Nodes : Node 9 , Node 28

If node is replicating the ip address of another node then same msg to be created for both nodes by MD5. Hence both nodes will be tested with their flags where node 1 & 2 will be true and node 9 & 23 will be false. Node 9 and 28 are defined as attackers since they replicate ip address shown clearly with same msg been created using MD5

Routing Node **Signature**

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

N1 c4dfd145e649849eb4a66f83c052a8de - Secured Node
N9 c4dfd145e649849eb4a66f83c052a8de - Replicated as N1
N28 a9913d1a1eaccaa08606200dc92faaac - Replicated as N2
N2 a9913d1a1eaccaa08606200dc92faaac - Secured Node

Fig. 5. shows the snapshot of the simulation where node 9 and node 28 are marked as attackers because they replicate ip address.

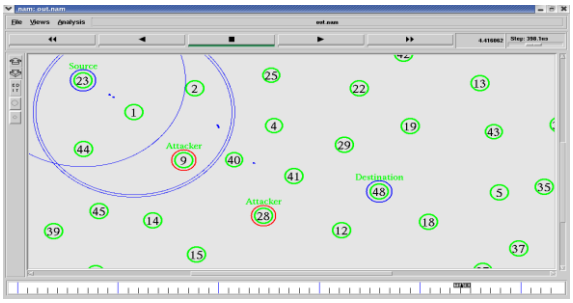

Fig. 5 Snapshot showing attacker in routing path

The values obtained using traditional AODV and proposed SE-AODV at different node sizes are listed in Table. 2. The traditional AODV doesn't provide reliable routing since the nodes present in the network drop packets while routing which degrades the performance of routing and results in reduced packet delivery ratio and increased delay.

Node Size	General AODV			Proposed SE-AODV		
	PDR	Delay	Throughput	PDR	Delay	Throughput
25	46.10	0.4430	757771.4	69.1	0.29538	75777
50	62.25	0.2615	120032.6	80.0	0.20340	12003
100	70.59	0.1822	115783.2	87.2	0.15595	11578
200	79.35	0.1558	113259.5	91.5	0.13759	11325
300	81.73	0.1263	110935.7	93.7	0.11925	11093

Table.2. Result comparison with different node sizes

The Qos parameter values are showing better improvement when the routing takes place with the proposed SE-AODV protocol which works using energy values that identifies untrustworthy nodes in the route and immediately take an alternate path to provide trustworthy and successfully routing. The results shown in the result comparison table clearly shows the PDR and delay increases as number of nodes increases (success rate higher as number of nodes increases) and throughput maintained (since in both cases transmission are similar).

Fig. 6. specifies the increase in PDR by implementing the proposed SE-AODV protocol compared to the traditional AODV protocol. Fig. 7. specifies the decrease in delay while using the proposed SE-AODV compared to traditional AODV

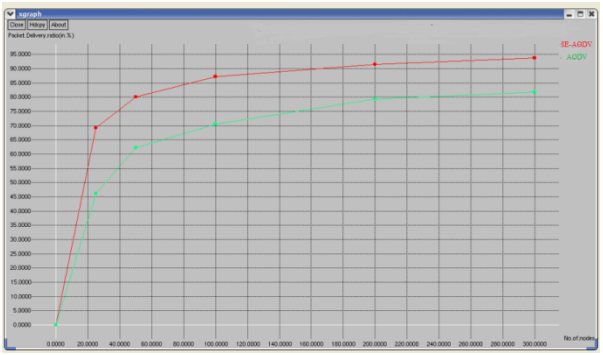

Fig. 6 Comparison of general AODV PDR and SE-AODV PDR

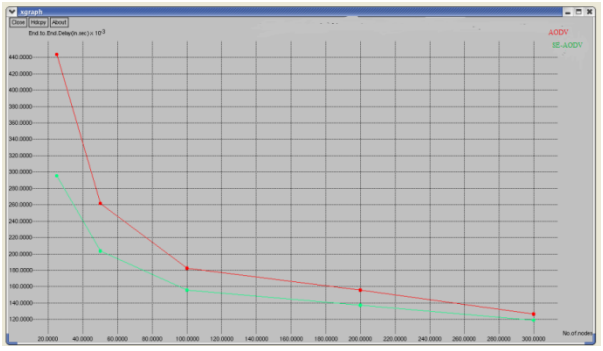

Fig. 7 Comparison of general AODV Delay and SE-AODV Delay

5. Conclusion and Future Enhancements

SE-AODV protocol is proposed that identifies the nodes that drop packets during data transmission. Energy value for each node is calculated to spot the untrustworthy nodes in the path during routing. A node is declared as a trustworthy node if its energy value is greater than the threshold value thus resulting in a trustworthy MANET routing. Every transmission is secured using Message Digest algorithm which is also used to identify attackers in routing path. This proposed scheme has shown a good development over Qos parameters like PDR and delay and has also provided trustworthy routing. The same scheme can also be implemented on other MANET routing protocols and check the performance with respect to Qos parameters. The future work may provide an new encryption scheme for secured packet transmission and also to consider virtual energy concepts for the nodes participating in the routing to enhance reliability in MANET routing.

ISSN 2394 - 7179 (Print)
ISSN 2394 - 7187 (Online)

References

[1] Kortuem.G., Schneider. J., Preuitt.D, Thompson .T.G.C, F'ickas.S. Segall.Z.: When Peer to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks. 1st International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001)

[2] P Narayan, V R. Syrotiuk.: Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool. In: the proceeding of ADHOC-NOW in the year of 2004.

[3] Charles E. Perkins, Elizabeth M. Belding Royer and Samir R. Das.: Ad-hoc On-Demand Distance Vector (AODV) Routing. Mobile Adhoc Networking Working Group, Internet Draft, February 2003

[4] I. Jawhar, and J. Wu: Quality of Service Routing in Mobile Ad Hoc Networks, in M Cardei, I Cardei & DZ Du (eds), Resource Management and Wireless Networking, Kluwer Academic Publishers.

[5] Pushpa, A.M.: Trust based secure routing in AODV routing protocol. In: IEEE International Conference (2009)

[6] Hothefa Sh.Jassim, Salman Yussof.: A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network. In: IEEE 9th Malaysia International Conference on Communications (2009)

[7] Mangrulkar, R.S.; Atique, M.: Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network. In: Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), 2010 .

[8] R. S. Mangrulkar, Dr. Mohammad Atique.: Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network. 2010

[9] Sharma, S.; Mishra, R.; Kaur, I.: New trust based security approach for ad-hoc networks. In: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[10] Umuhoza, D, Agbinya, J.I, Omlin, C.W.: Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007.

[11] Ferdous, R., Muthukkumarasamy, V., Sattar, A.: Trust Management Scheme for Mobile Ad-Hoc Networks. In: IEEE 10th International Conference on Computer and Information Technology (CIT), 2010.

Sridhar Subramanian Received the B.Sc. degree from the University of Madras, Chennai, India, Master of Computer Applications (MCA) degree from University of Madras, Chennai, India, Master of Philosophy (M.Phil.) degree from Periyar University, Salem, Tamil Nadu, India and pursuing Ph.D. (Computer Science) in Barathiyar University, Coimbatore, Tamil Nadu, India. Currently employed in the Department of Computer Applications, S.A. Engineering College, Chennai as Associate Professor. The area of research is Qos routing in Mobile Ad hoc networks.