A Trust-Based Scheme against Packet Dropping Attacks in MANETs

Sachi N. Shah
Department of Computer Engineering
SVM Institute of technology
Bharuch 392-001, Gujarat, India
sachi20shah@gmail.com

Rutvij H. Jhaveri
Department of Computer Engineering
SVM Institute of technology
Bharuch 392-001, Gujarat, India
rhj_svmit@yahoo.com

***Abstract*— Mobile Ad-hoc Network (MANET) is a dynamic network topology in which nodes move without restraint anytime and anywhere; it does not require centralized authorization. Previous researches used traditional cryptographic or authentication function for security. Recently many trust-based routing protocols have been introduced but each has its own limitations. In MANETs, trust is a challenging task. In this network, it is imperative for the nodes to work in a trusted and cooperative way. This paper proposed a new secure trust based routing scheme which is combination of social and QoS trust. The primary goal of our proposed scheme is to mitigate nodes performing various packet forwarding misbehaviors. We calculated four parameters for trust which are control forward ratio, data forward ratio, intimacy and residual energy. We present adversary model of the packet dropping attack against which our trust-based scheme is evaluated. Simulation results in NS-2 show that the proposed scheme improves performance in terms of packet delivery ratio (PDR).**

***Index Terms*— MANET, Routing, Trust-based scheme, Packet forwarding misbehavior, AODV.**

I. INTRODUCTION

We focus in term Mobile Ad-Hoc Networks (MANET) to refer Dynamic, Infrastructure less, Self configuring network consisting of wireless mobile nodes that communicate with one another via radio waves and while not use of any centralize authority. In MANET all nodes are behaving either as router or Participate node [1]. Nodes are free from charge from any central authority to maneuver everyplace within the network, who comes in radio range of each other will communicate directly and who not comes in range of each other will communicate with the help of intermediary nodes[2].

There are various difficult problems in MANETs like Limited bandwidth, Dynamic nature of topology, Routing Overhead of network, Packet losses, Route changes, Battery constraints, Security threats, Device discovery, Quality of Service (QoS) and Inter-networking. Civilian environments, Emergency operations, Military battlefield, Collaborative work, Local level, Personal area network and Bluetooth, Commercial Sector, are applications of MANET[2] [3].

The process of routing is choosing best path from sender node (source) to destination node (destination) for communication. Route calculation is needed before established the route or once it required. Routing has 2 activities: (1) Route discovery and (2) Packet forwarding. In Route discovery part shortest and best path is established and acknowledge between source to destination and In Packet forwarding part source node sending packets to destination node with or without facilitate of intermediate node [1] [4].

Figure 1 shows routing protocols [8]. Routing protocols classified as follow: (1) Proactive routing Protocol (2) Reactive routing Protocol (3) Hybrid routing Protocol. Destination-Sequenced Distance Vector routing (DSDV), Optimized Link State Routing Protocol (OLSR), and Fisheye State Routing (FSR) are example of Proactive routing Protocol that is additionally known as table driven routing protocol. Dynamic source Routing protocol (DSR), Ad hoc On Demand Distance Vector routing protocol (AODV) [19],[20], Temporally Ordered Routing Protocol (TORA) are example of Reactive routing protocols that is additionally known as on-demand routing protocols. Hybrid protocols are combination of Reactive and Proactive routing protocols. Zone Routing Protocol (ZRP) is example of it [2], [4], [5], [6], [7], [8].We are focusing in Reactive routing protocol for our examination that is AODV protocol.

Trust is incredibly vital think about social science engineering. Security is incredibly vital side for any ad hoc network that never comprises at any level. Security and trust are co-related with one another. If trust level augmented security should be increase [9]. Definition of trust is totally different for each discipline. In Ad-hoc Network, Trust is outlined as “Relations between entities that participate during a protocol”. In alternative words, we will say that “The level of belief regarding the behavior of alternative entities” [10].

There are two sorts of trust: (1) Social trust, (2) QoS trust. Social trust obtained from social relationships. Friendship, Honesty, Privacy and Intimacy are example of social trust. Qos trust obtained from competency, dependability, reliability, successful experience, number of forward packets and data packets [10]. Subjectivity, Dynamicity, Asymmetry, incomplete transitivity, context-dependency are properties of trust [10][11][12]. Trust will be invariably live between the worth [0, 1]. If trust value of node is zero than node isn't trustworthy and if trust value of node is one than node is trustworthy node [12]. In MANET trust will be achieves by varied Trust Models [13].

The rest of Paper is organized as follow. In Section 2 mention related works on trust based approaches in MANET. Section 3 focused on the design of our new secure trust based routing protocol and Adversary model. Section 4 presents simulation parameters. Section 5 presents simulation results of trust based secure routing model against adversary model and its evaluation. In Final section Paper is concluded.

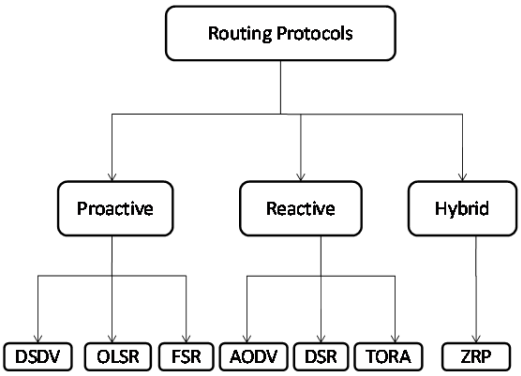


Fig. 1. Routing Protocols in MANET

II. Related Work

We have carried out literature survey on the various trust based secure routing protocol which are described as follows:

Subramaniam et.al [5] Presents Trust based AODV protocol. In this paper node selection process performs before routing. Trust and energy are measured before nodes are chosen for routing and threshold value is outlined clearly. Node's trust and energy levels are beyond threshold for considering it in routing process.

Kukreja et.al [6] took Dynamic source Routing Protocol (DSR) as main protocol and extends it and named as Energy Efficient Secure Dynamic source Routing (EESDSR). For detection of malicious node they used distributed trust model. Chosen path isn't continuously shortest path however it's trustiness and free from malicious node. EESDR operating in five phases: phase I: Selection of monitor nodes phase II: Trust Model phase III: Monitoring of nodes' behavior and trust update phase IV: Trust Propagation phase V: Route Selection.

Tan et.al [14] extends the OSLR protocol with projected trust model and trust routing algorithm referred to as FPNT-OSLR. Trust reasoning model is employed for calculate trustworthiness of nodes and trust routing algorithm is employed to seek out most trustworthy path between two nodes among several possible paths within the networks. A combination classical Petri net and fuzzy logic is named fuzzy petri net.

Estahbanati et.al [15] projected Hidden markov model (HMM) as trust model that relies on Markov chain trust. The main focus of the paper is for choosing the suitable route they measured the trust value of the node furthermore the available energy of the node. Within the network source node calculate trust value of other nodes.

Sarkar et.al [16] planned Secure and Energy-Efficient Stochastic (SEES) protocol. First they concentrate on routing problem as stochastic routing that is resolved supported a Markov chain model of trust. Second they used Bellman's Principle of Optimality Equation for optimize value function in terms of current packet forwarding energy consumption and future packet forwarding energy consumption.

Biswas et.al [17] projected a solution for detect and prevent black hole attacks for each single and co-operative node with making certain secure packet transmission. Within the network every node have three parameter for checking its trust (1) Rank, (2) Remaining Battery power and (3) Stability issue. If the rank of the node is falls zero than take into account it as black hole node. This projected scheme applied once after route discovery section and minimum rank thought is 1.

III. PROPOSED WORK

A. Adversary Model

For Packet dropping attack we tend to design adversary model. In packet dropping attack, offender node reply positively to route whether it is not fresh or valid route within the direction of destination. Packet dropping attack happens at the time of routing the data packet. As a result of this all neighborhood traffic diverted to offender node ensuing it drops all the packets. In scenario it's not fully gray hole attack however partially gray hole attack. Figure 2 and Figure 3 shows adversary model [18].

B. Trust Based Secure Routing Model

We have carried out four mechanisms for trust calculation, trust update and isolation of malicious node.

(1) HELLO message exchange
(2) Promiscuous mode monitoring
(3) Trust update mechanism
(4) Isolating of malicious node

Figure 4 shows the flowchart for HELLO message exchange. In first mechanism every node broadcast hello message periodically with residual energy of current node. If the node who sends hello message is trusted node than calculate the intimacy of sending node with interacted neighbor node. Intimacy is defined that at the same time which node's interaction is higher with sender node.

In second mechanism Promiscuous mode monitoring is performed. In Promiscuous mode each node in the network listens the packets transmitted by its own neighbor nodes. Node A wants to monitor the packets from a node B in promiscuous mode to check whether node B is forwarding the packets which are sent by A to B or not.

Figure 5 shows the flowchart for Trust update mechanism. We will calculate trust with below formula:

Neighbor_Trust=w1*CFR+w2*+DFR+w3*Energylevel+ w4*Intimacy level (1)

(Where 0<w1, w2, w3, w4<1 and w1+w2+w3+w4 =1)

Here w1, w2, w3, w4 are weighted factor and CFR as control forward ratio and DFR as data forward ratio initially

we will think to take value of w1, w2, w3, w4 as 0.25 and threshold value as 0.7.

Figure 6 shows flowchart for Isolating of malicious node. In forth mechanism isolates the control packets received from malicious node.

IV. SIMULATION PARAMETERS

The simulation parameter is explained as below which is used to generate the simulation results for adversary models and proposed solution.

We used NS-2.34 as Simulator with 1000X1000 scenario size. Number of nodes, Misbehaving nodes and mobility vary for simulation results. Packet size is taken 512 bytes. Simulation time is 240sec. we used performance metrics such as Packet delivery ratio, End-to-End delay and Routing overhead.

TABLE I. SIMULATION PARAMETERS

Parameter	**Values**
Simulator	NS 2.34
Routing Protocol	AODV, Packet Dropper, Trust based secure routing protocol
Scenario Size	1000X1000
Number of Nodes	20,40,50, 60,80,100
Misbehaving Nodes	0,2,4,6,8
Simulation Time	240 sec
Traffic Type	Constant Bit Rate (CBR) / UDP
Packet Size	512 bytes
Number of connections	5
Packet Rate	4 packets/sec
Pause Time	5 sec
Maximum Speed	5,10,15,20,25 m/sec

Procedure 1: Actions by the malicious node after receiving RREQ from the source node

If (RREQ is not for me) **then**

Received RREQ will be discard

// A random value between 1to 10 add to the RREQ Dest seqnno

RREP packet Fill up with Dest Seqno=RREQ Dest Seqno + Random number (1:10) and Hop count=2

Unicast the forged RREP on the reverse path to the source

Else

RREP packet Fill up with own Seqno and Hop count=1

Received RREQ will be discard

Unicast the genuine RREP on the reverse path to the source

End If

Fig. 2. Adversary Model

V.SIMULATION RESULTS

We conduct simulation results for 3 cases: Test 1: By varying Mobility, Test 2: By varying Attacker nodes, Test 3: By varying number of nodes. Here We show simulation results of Test 1 and Test2.

Graph (a) shows that Packet Delivery ratio of AODV under attack decrease with increase the mobility of node as compare to AODV protocol and after applying Trust based secure routing model PDR increase as compare to AODV under attack. **Graph(b)** shows that End –to-En d Delay of AODV under attack gradually decrease with increase the mobility as compare to AODV protocol. Due to position of nodes at some point it increases the result of AODV with trust. **Graph (c)** shows that Routing overhead of AODV under attack increase with the increasing the mobility of node as compare to AODV protocol and after applying trust model Routing overhead decrease as compare to AODV under attack. **Graph (d)** shows that Packet Delivery ratio of AODV with attack decrease with increasing number attacker nodes. At the point of 0 attacker

node means in normal AODV it gives higher PDR. After applying trust model it gives better result as compare to attack model. **Graph (e)** shows that End-to-End delay of AODV with attack decrease with increasing number of attacker nodes. At some point due to nodes position and mobility speed it gives high performance. After applying trust model End-to-End delay increase as compare to AODV under attack condition. **Graph (f)** shows that Routing overhead of AODV with attack gradually increase with increasing number of attacker nodes and as compare to AODV under attack condition Routing overhead decrease after applying trust model.

Procedure 2: Actions by the malicious node after receiving data packets from the source node

If (Current Time > time1 && Current Time <=time2) then //time2-time1=50% time period

The data packet received from the source will be drop

Else

if a valid route is available the data packet will be Forward

End If

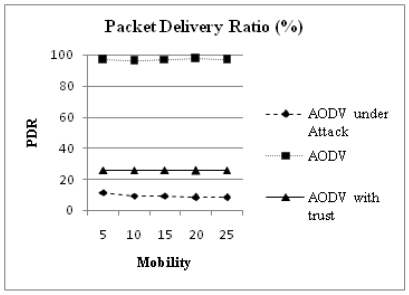
Else

Receive the data packet for me

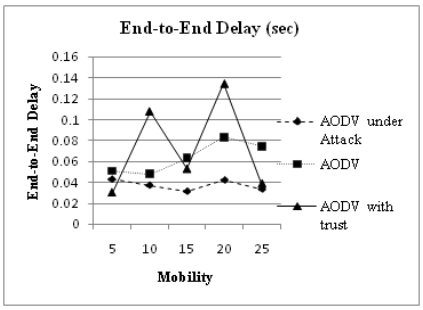
End If

Fig. 3. Adversary Model

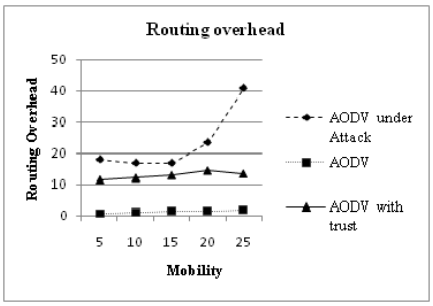
Test 1: By Varying Mobility



(a) PDR vs Mobility

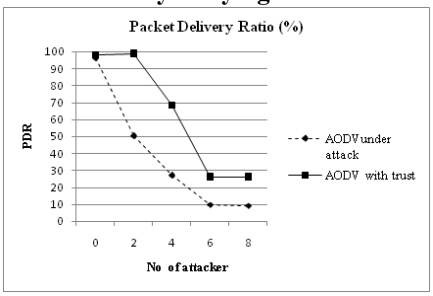


(b) End-to-End Delay vs Mobility



(c) Routing overhead vs Mobility

Test 2: By Varying attacker node



(d) PDR vs No of attacker

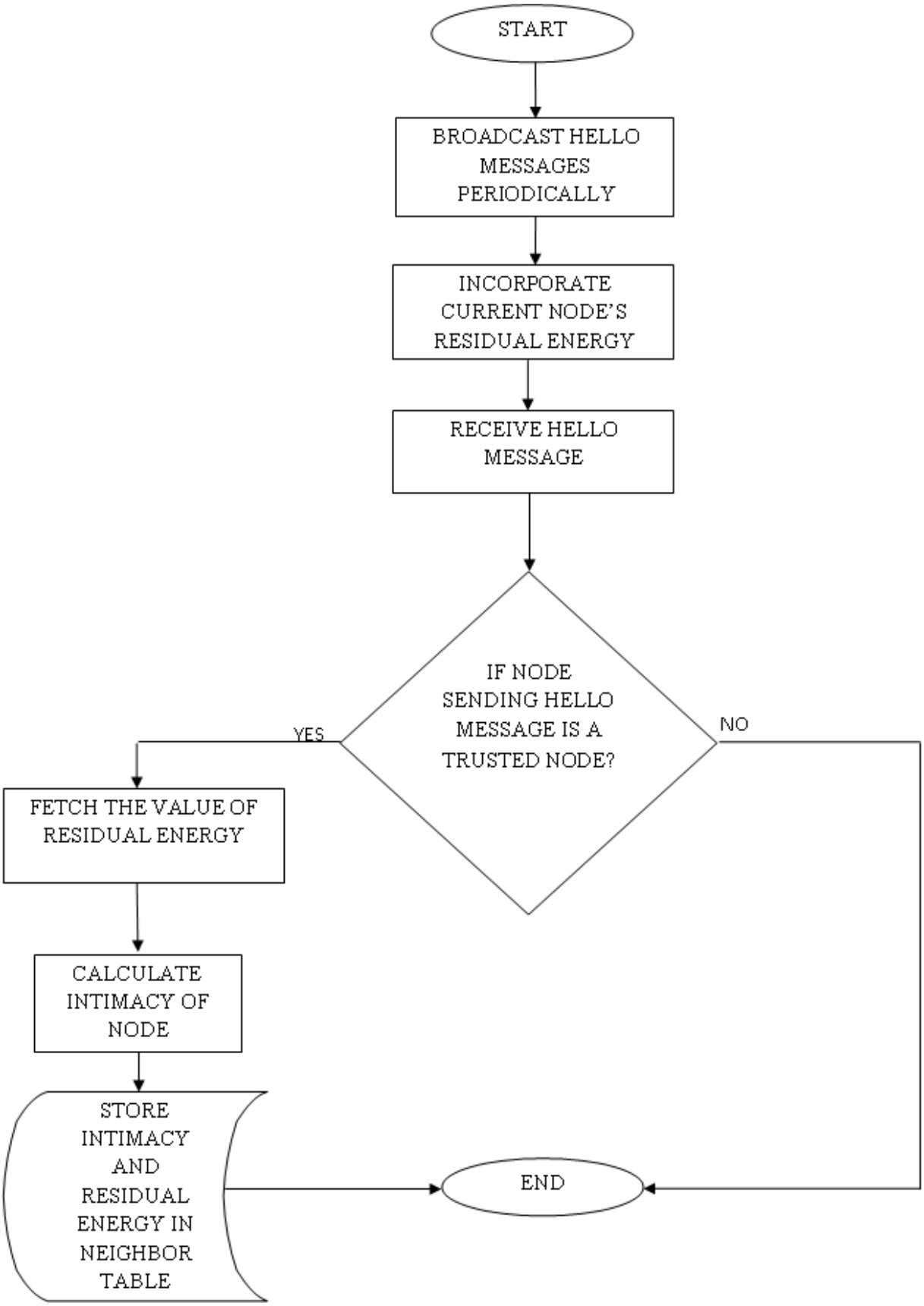


Fig. 4. HELLO Message Exchange

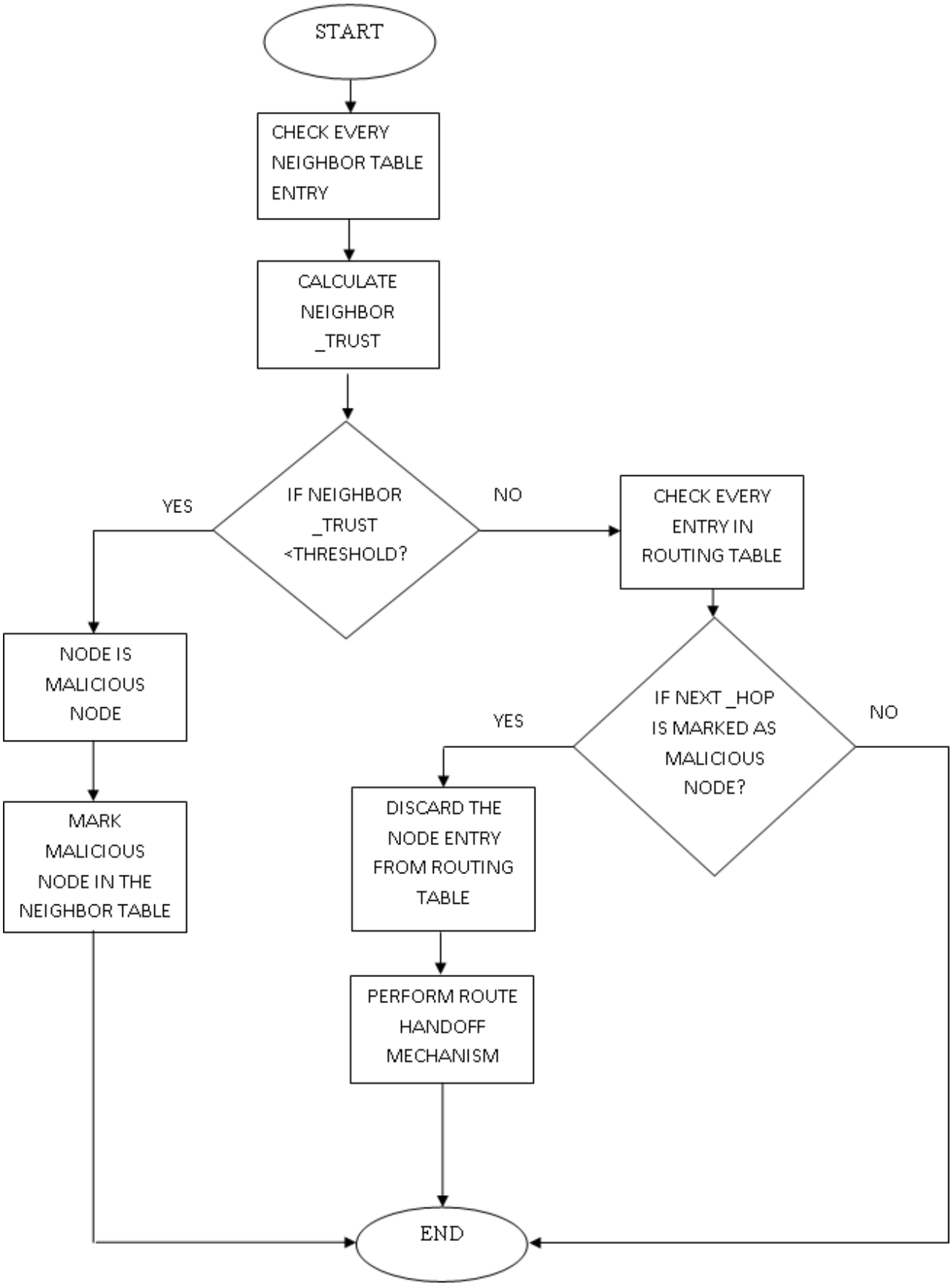


Fig. 5. Trust Update Mechanism

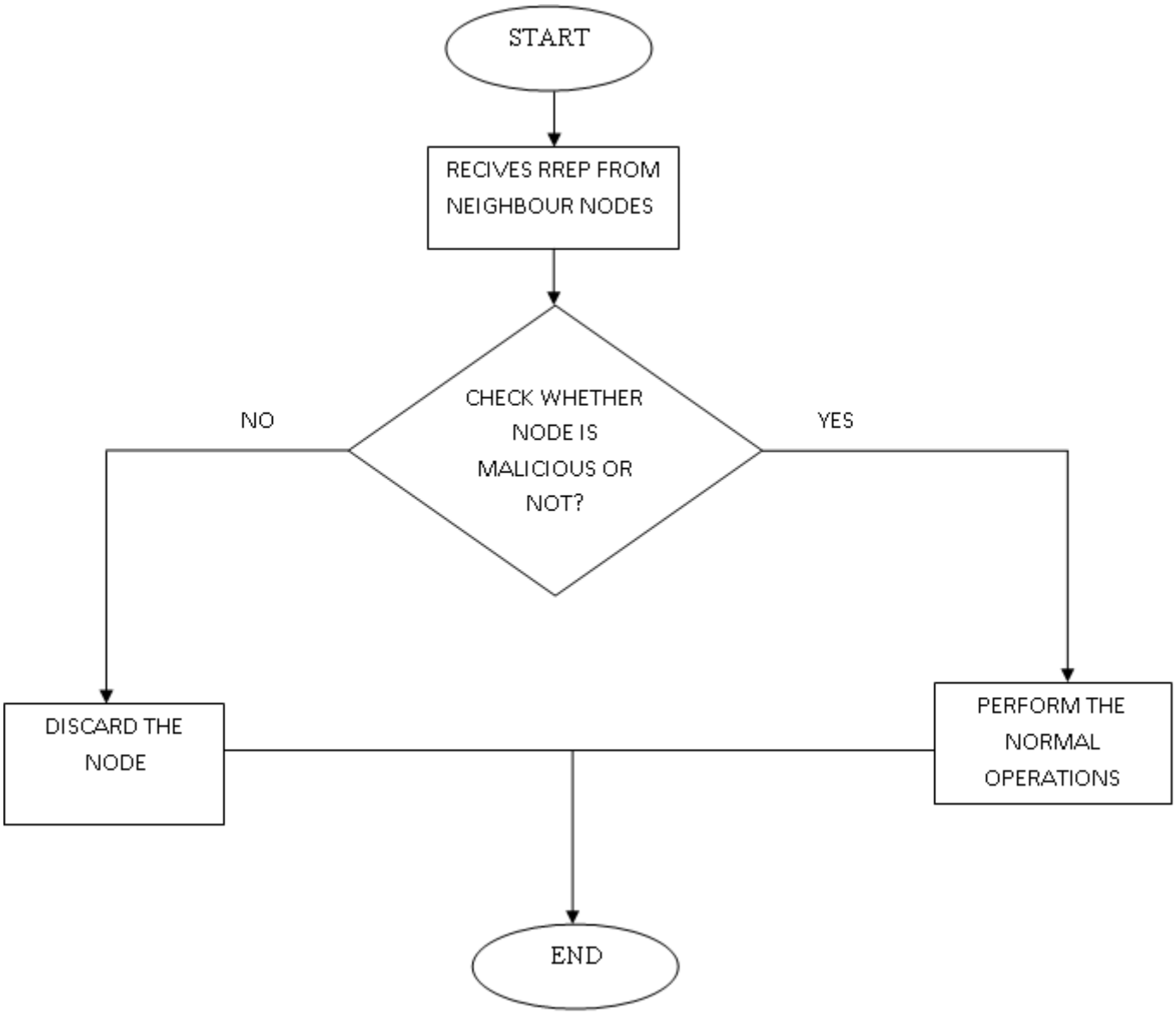
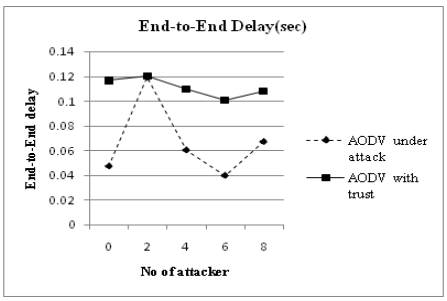
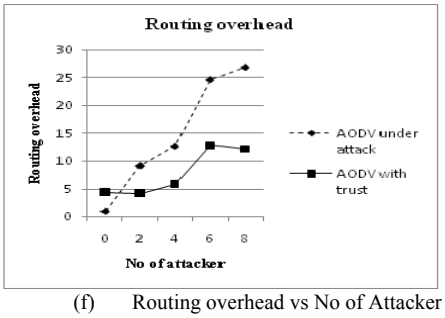


Fig. 6. Isolating of Malicious node



(e) End-to-End Delay vs No of Attacker



(f) Routing overhead vs No of Attacker

VI. CONCLUSION AND FUTURE WORK

Trust and security are two sides of a coin as they are interconnected with each other. Both are very important aspects of any ad hoc network. This paper proposed a trust-based scheme which combines

social and QoS trust. We evaluate AODV protocol against an adversary model and also with our proposed model. We also analyze theoretically our scheme against the adversary model. Under attack condition, AODV provides significant fall in packet delivery ratio as compared to normal AODV protocol. We show that our proposed model would give improved in terms of packet delivery ratio. In future, for better network performance add social trust parameter like friendship, honesty and give physical interpretation to the terms in weighted sum formula as check with different value of w1 to w4 and check the improvements in result.

REFERENCES

[1] Kumar, Narendra. "Battery power and trust based routing strategy for MANET." In *Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on*, pp. 1559-1562. IEEE, 2014.

[2] Aarti, Dr SS. "Tyagi, Study of MANET: Characteristics, Challenges, Application and Security Attacks." *International Journal of Advanced Research in Computer Science and Software Engineering* 3, no. 5 (2013): 252-257.

[3] Bang, Ankur O., and Prabhakar L. Ramteke. "MANET: history, challenges and applications." *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2, no. 9 (2013): 249-251.

[4] Shah, Sachi N., and Rutvij H. Jhaveri. "A survey of various energy efficient secure routing approaches for wireless ad-hoc networks." In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, pp. 1424-1429. IEEE, 2015.

[5] Subramaniam, Sridhar, and Baskaran Ramachandran. "Energy- and Trust-Based AODV for Quality-of-Service Affirmation in MANETs." In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, pp. 601-607. Springer India, 2015.

[6] Kukreja, Deepika, Sanjay Kumar Dhurandher, and B. V. R. Reddy. "Enhancing the Security of Dynamic Source Routing Protocol Using Energy Aware and Distributed Trust Mechanism in MANETs." In *Intelligent Distributed Computing*, pp. 83-94. Springer International Publishing, 2015.

[7] Mittal, Shaily, and Prabhjot Kaur. "Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET's." In *2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pp. 165-168. IEEE, 2009.

[8] Fonseca, Emanuel, and Andreas Festag. "A survey of existing approaches for secure ad hoc routing and their applicability to VANETS." *NEC network laboratories* 28 (2006): 1-28.

[9] Pirzada, Asad Amir, and Chris McDonald. "Establishing trust in pure ad-hoc networks." In *Proceedings of the 27th Australasian conference on Computer science-Volume 26*, pp. 47-54. Australian Computer Society, Inc., 2004.

[10] Ramana, K. Seshadri. "ASurvey ON TRUST MANAGEMENT FOR MOBILE AD HOC NETWORKS.“

[11] Cho, Jin-Hee, Ananthram Swami, and Ing-Ray Chen. "A survey on trust management for mobile ad hoc networks." *Communications Surveys & Tutorials, IEEE* 13, no. 4 (2011): 562-583.

[12] Vijayan, R., and N. Jeyanthi. "A Survey of Trust Management in Mobile Ad hoc Networks." *International Journal of Applied Engineering Research* 11, no. 4 (2016): 2833-2838.

[13] Dalal, Renu, Manju Khari, and Yudhvir Singh. "Different ways to achieve Trust in MANET." *International Journal on AdHoc Networking Systems (IJANS) Vol* 2 (2012).

[14] Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "Trust based routing mechanism for securing OSLR-based MANET." *Ad Hoc Networks* 30 (2015): 84-98.

[15] Estahbanati, Maryam Miri, Mehdi Rasti, and Seyyed Mostafa Safavi Hamami. "A mobile ad hoc network routing based on energy and Markov chain trust." In *Telecommunications (IST), 2014 7th International Symposium on*, pp. 596-601. IEEE, 2014.

[16] Sarkar, Sajal, and Raja Datta. "A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks." In *2014 Twentieth National Conference on Communications (NCC)*.

[17] Biswas, Santosh, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." In *Applications and Innovations in Mobile Computing (AIMoC), 2014*, pp. 157-164. IEEE, 2014.

[18] Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack.

[19] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[20] Jhaveri, Rutvij H., and Narendra M. Patel. "Mobile Ad-hoc Networking with AODV: A Review." *INTERNATIONAL JOURNAL OF NEXT-GENERATION COMPUTING* 6, no. 3 (2015).