International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:9, No:3, 2015

Trust and Reputation Mechanism with Path Optimization in Multipath Routing

Ramya Dorai, M. Rajaram

***Abstract*—**A Mobile Adhoc Network (MANET) is a collection of mobile nodes that communicate with each other with wireless links and without pre-existing communication infrastructure. Routing is an important issue which impacts network performance. As MANETs lack central administration and prior organization, their security concerns are different from those of conventional networks. Wireless links make MANETs susceptible to attacks. This study proposes a new trust mechanism to mitigate wormhole attack in MANETs. Different optimization techniques find available optimal path from source to destination. This study extends trust and reputation to an improved link quality and channel utilization based Adhoc On-demand Multipath Distance Vector (AOMDV). Differential Evolution (DE) is used for optimization.

***Keywords*—**Mobile Adhoc Network (MANET), Adhoc On-demand Multi-Path Distance Vector (AOMDV), Trust and Reputation, Differential Evolution (DE), Link Quality, Channel Utilization.

I. Introduction

MANET a self-organized, decentralized wireless network with core mobility functionality is adhoc because it is built unexpectedly as devices are connected, and so determining which nodes forward data is based on network connectivity [1]. This is contrary to wired networks where routers perform routing. It is different from managed (infrastructure) wireless networks where a special node called access point manages inter-node communication.

Routing protocols establish connections and route data packets for which control signals and data signals are used. They are categorized according to properties: Proactive and Reactive routing protocol. Proactive routing protocol is table driven where routing table is updated when change occurs in network topology. Mobile nodes are dynamic and hence proactive routing protocols are not useful in dynamic topologies [2]. Reactive routing protocol is an on-demand routing protocol where, when a source wants to forward a data packet it establishes a connection. It uses route discovery to connect, and route maintenance to maintain broken links.

Presently, multipath routing is also considered. Multipath routing allows establishing of multiple paths between source and destination nodes to increase data transmission reliability and ensure load balancing. Multiple paths amongst source and destination node pairs compensate for MANETs dynamic and unpredictable nature supporting Quality of Service (QoS).

Ramya Dorai is with Adhiyamaan College of Engineering, Hosur, Tamilnadu, India (e-mail: ramyadorai.aom@gmail.com).

Rajaram. M is Vice-chancellor, Anna University, Chennai, Tamilnadu, India.

Multipath based routing protocols discover node disjoint, link-disjoint or non-disjoint routes. Node disjoint routes called totally disjoint routes have no nodes or links in common. Non-disjoint routes have lower aggregate resources than disjoint routes, as non-disjoint routes share links or node. Non-disjoint routes advantage is that they are easily discovered as there are no restrictions requiring routes to be node or link-disjoint. Only paths subset satisfying QoS requirements are selected [3] in QoS routing.

Many multipath routing protocols are suggested for adhoc networks to provide reliable communication, ensure load balancing and improve adhoc and mobile networks QoS. Multipath routing protocols improve delay, reduce overhead, and maximize network life. Multiple paths are used as backup route or are used simultaneously for parallel data transmission (like round robin).

Most multipath protocols are reactive routing protocol based (Adhoc On-demand Distance Vector routing (AODV) or Dynamic Source Routing (DSR)). Reactive multipath routing protocols improve network performance but also have disadvantages [4]:

- Route request storm: Multipath reactive routing protocols generate route request messages. When intermediate nodes process duplicate request messages, redundant overhead packets are introduced in the networks.
- Inefficient route discovery: Some multipath routing protocols prevent intermediate nodes from replying from its route cache to find node-disjoint or link-disjoint paths.

They directly attack network to delete messages, inject false packets or impersonate nodes. This violates network goals of authentication, availability, integrity, and non-repudiation. Compromised nodes attack from within the network. MANET security involves authentication, key establishment, distribution, and encryption. Routing protocols assume pre-existence and pre-sharing of public and secret keys for initial members [5]. The protocols neglect key exchange and authentication, important in MANETs.

MANET security provides availability, confidentiality, integrity, authorization, authenticity, and anonymity [6]. For secure information transmission, MANET communication security is important. Absence of a central co-ordination mechanism and shared wireless medium makes MANET vulnerable to digital and cyber-attacks than wired networks. Many attacks affect MANETs, and they are classified as two types [7]:

1. External Attack: External attacks are by nodes not of the network. It sends false routing information, causes congestion, or services unavailability.

2. Internal Attack: Internal attacks are by compromised network nodes. In internal attacks, a malicious network node gains unauthorized access and impersonates a genuine node. It analyzes traffic between nodes and participates in network activities.

Denial of Service (DoS) attacks is most worrying for network managers. In a military environment, such attacks are extremely dangerous, and engineering such attacks is a modern war-goal [8]. MANETs security goals can change in different modes (e.g. peace time, transition to war, and a military network's war time). MANETs characteristics make them susceptible to new attacks. Top level attacks are classified according to network protocol stacks.

TABLE I
ATTACKS ON THE PROTOCOL STACK

Layer	Attacks
Application Layer	data corruption, viruses, and worms
Transport Layer	TCP/UDP SYN flood
Network Layer	hello flood, blackhole
Data Link Layer	monitoring, traffic analysis
Physical Layer	eavesdropping, active interference

Trust is a degree of belief about other entities behavior. Nodes participating in data exchange should be shielded by trust and reputation mechanisms, or they can be attacked ending in the network's unnecessary resource consumption. Attacks can be direct or indirect, i.e., intruders might take charge of good nodes resulting in non-cooperation leading to network destruction. So, compromise prone nodes should be identified via trust and reputation mechanisms in advance to ensure network safety. A trust agent derives trust levels from events directly experienced by a node. A Reputation agent shares nodes trust information about nodes with other network nodes. A Combiner computes final node trust based on information received from Trust and Reputation agents. Trust computation is through direct and indirect information [9], [10].

Trust value is propagated by piggybacking nodes direct trust value with RREQ packets. Every time a packet is forwarded, forwarding node scans routing tables for alternate destination paths. It compares all next hops direct trust value in the path and selects one with highest trust value. A trust-aware routing component should [11]:

- Exploit trusted paths for routing traffic, i.e., for paths with unambiguous trustworthiness measures, decision maker routes traffic without subjective judgment.
- Penalize stations not conforming to packet forwarding protocol.

Exploitable paths are those which a route decision maker categorizes as trusted or mistrusted enabling an optimization approach that is not specific to a trustworthiness measure. This study extends previous work's trust and reputation to improved AOMDV based on link quality and channel use. Section II reviews related work. Section III explains methodology. Section IV discusses experimental results, and Section V concludes the work.

II. Related Works

A trust protocol based on congestion control was presented by [12] where congestion control section guarantees network stability and distributes load on most highly trust nodes. The model was performed by agents on network nodes. To show the model's probability, it uses the AODV protocol. Regarding simulation on OPNET environment, the model improved network efficiency though trust was affected by malicious nodes and network congestion.

A reputation-based trust management system to detect and prevent MANET vulnerabilities was proposed by [13]. Active (malicious nodes) and passive (selfish nodes) attacks were investigated; the new scheme aid nodes to exclude them from network while tolerating transient faults. The scheme works with on-demand routing protocols. The proposed scheme's performance was evaluated in a discrete event-simulation environment, and results indicated scalability and robustness.

A trustworthy path discovery in MANET comprising an effective reputation based trust management scheme through monitored traffic cross-correlation and a trust based routing protocol that evaluates trustworthy path dynamically was presented by [14]. Analysis revealed major improvement in AODV packet delivery ratio during attacks, with marginal control traffic overhead rise.

Extending AODV and AOMDV routing protocol, [15] proposed a new Adhoc On-demand Trusted-path Distance Vector (AOTDV) for MANETs. The new protocol discovers multiple loop-free paths as candidates in a route discovery which are evaluated in two aspects: hop counts and trust values. Experiments compared the protocols, and results showed that AOTDV improved packet delivery ratio and mitigated black hole, grey hole, and modification attack impairment.

A light-weight trust-based routing protocol was presented by [16]. It is light-weight in that; Intrusion Detection System (IDS) is used to estimate the trust one node has for another, consuming limited computational resource. It also uses local information ensuring scalability. The proposed light-weight IDS takes care of two kinds of attacks: blackhole attack and grey hole attack.

A QoS enabled Ant colony-based Multipath Routing (QAMR) algorithm based on the ant colony's foraging behaviour to select a path and transmit data was proposed by [17] where path is selected based on nodes stability and path preference probability. The authors considered bandwidth, delay, and hop count as QoS parameters and also, node stability, hops number, and path preference probability factors. Simulations with NS2 showed the new algorithm to be scalable and performed better at higher traffic load compared to current algorithms.

A MANETs message security approach using a trust-based multipath AOMDV routing combined with soft-encryption, yielding T-AOMDV scheme was proposed by [18]. Simulation with NS2 proved that the new scheme is more secure than conventional multipath routing algorithms with a recently proposed MANETs message security scheme (trust-based Multipath Routing scheme (T-DSR)), being the

benchmark. Route selection time and trust compromise are the performance criteria used.

A light-weight trust-based multipath routing protocol called LWT-AOMDV based on a new model, extending from AOMDV was proposed by [19]. The proposed work's key issue is establishing multiple trustworthy paths and timely detection of malicious nodes. This protocol's on-demand route maintenance mechanism reduced control overhead by presenting path error notion instead of route error. A new protocol explored tradeoff between overhead and service quality. Simulation via NS2 simulator proved that the new approach improved packet delivery ratio at the expense of additional resources.

An Adaptive Secured Multipath for Adhoc networks (ASMA) as a scalable, flexible and application-oriented framework able to manage security based on application requirements and network security conditions was proposed by [20]. ASMA is based on a macrograph structure combining dynamic trust management and multipath routing. ASMA simulation results were associated with AOMDV (a multipath declination of AODV) routing protocol and compared with AOMDV. Results revealed that ASMA-AOMDV outperformed AOMDV, dividing by three networks packet loss rate including 20% malicious nodes while causing only 3% additional loss in safe networks.

A trust based collaborative approach to lessen blackhole nodes in AODV protocol for MANET was presented by [21] where every node monitors neighbouring nodes to calculate trust value on them dynamically. If a monitored node's trust value is lower than a predefined threshold, then monitoring node assumes it as malicious and avoids it on route path. Experiments revealed that the new scheme secured AODV routing protocol for MANET by avoiding blackhole nodes.

A security-enhanced AODV routing protocol called Reliant AODV (R-AODV) was presented by [22]. The proposed work's implementation is done by modifying a trust mechanism called direct and recommendations trust model and incorporating it inside AODV which allows it to find shortest path that is trusted. R-AODV protocol was implemented and simulated on NS2. Based on result, R-AODV provides a more reliable data transfer compared to normal AODV during malicious nodes presence in MANETs.

III. Methodology

This work extends trust and reputation of previous work to an improved AOMDV based on link quality and channel use. Differential Evolution (DE) is used for trust value (delta and mu) optimization.

A. Adhoc On-demand Multipath Distance Vector Routing (AOMDV)

AOMDV protocol is an AODV protocol extension for computing multiple loop-free and link-disjoint paths. Each destination's routing entries have a list of next-hops with corresponding hop counts. All next hops have same sequence number which helps track a route.

A node maintains advertised hop count for each destination, defined as maximum hop count for all paths used to send destination route advertisements. A source node floods a RREQ to network to find destination routes, and when destination node receives RREQ via different neighbors, it transmits multiple Route Reply (RREP) packets to source node. When the destination node replies RREP packets to source, intermediate nodes add current battery status to sum of field battery capacity in RREP packet to select data transmission route.

When intermediate nodes residual battery comes under the threshold, they flood RREQ packets and source node switches to another route among candidates to extend network life [23], [24]. AOMDV protocol ensures a route recovery mechanism when a link in an active route breaks to reduce lost packets. The AOMDV protocol's core is in ensuring that multiple paths discovered are loop-free and disjoint, and in efficiently locating paths using a flood-based route discovery. AOMDV route updates rules applied at each node locally and plays a key role in maintaining loop-freedom and disjointness properties.

AOMDV relies on the routing information available in underlying AODV protocol, thus limiting overhead due to discovering multiple paths [25]. It does not use special control packets. But, extra RREPs and RERRs for multipath discovery and maintenance with a few extra fields in routing control packets (RREQs, RREPs, and RERRs) are the only additional AOMDV overhead relative to AODV.

Link Quality

Each network node estimates its links quality with its one-hop neighbors. If Nq is number of HELLO packets received in a time window T_{win} and Pq are the percentage of HELLO packets received in last r seconds, then link quality Lq is measured as [26]

$$Lq = d.Pq + (1-d).Nq \quad (1)$$

Estimated link quality is maintained by every node in its NT. Average quality of all links across path P gives route quality Rq of path. Reverse path RREQ packets and forward path RREP packets accumulate estimated Lq values.

Channel utilization

This network considers IEEE 802.11 MAC with Distributed Coordination Function (DCF). It has packet sequence as Request-To-Send (RTS), Clear-To-Send (CTS), data, and Acknowledgment (ACK). The time between receipt of one packet and transmission of the next is a Short Inter Frame Space (SIFS). Then channel occupation due to MAC contention will be

$$C_{occ} = t_{RTS} + t_{CTS} + 3t_{SIFS} + t_{acc} \quad (2)$$

where t_{RTS} and t_{CTS} are time consumed on *RTS* and *CTS*, respectively and t_{SIFS} is *SIFS* period. t_{acc} is time for access contention. Channel occupation depends on medium access

contention and number of packet collisions. That is; C_{occ} is strongly related to congestion around a given node. C_{occ} becomes relatively large if congestion is not controlled, and dramatically decrease congested link capacity.

B. Trust and Reputation

A distributed statistical profiling technique to filter RREQs (by destination) or RREPs (by source) with excessively large delays is proposed. As different RREQs take varying hops, upper bound is calculated on per hop RREQ/RREP packets time to retain normal packets and to filter false packets. Retransmit timeout (RTO) calculations by TCP that capture a connection's average and deviation of round trip times is calculated. A destination node filters (discards) RREQs targeted to it in this design of huge delays. Consider a route discovery from source *S* to destination *D*. *D* receives first copy of RREQ with hop count h_1 at local time t_1, and second RREQ copy with hop count h_2 at time t_2. Let t_0 denote destination local time when request originated at source. As actual value of t_0 is not known, how *D* estimates it, is seen below. RREQ with new sequence number is considered legitimate, and destination sends a RREP to source. For every duplicate RREQ received, destination calculates route Request Hop Time (RHT), time taken by request packet to reach destination divided by hop count as in (3). Destination computes smoothed average, denoted *avgRHT*, and deviation, *devRHT*, of RHT for accepted RREQs, as in (5) and (6). To distinguish between malicious route requests and normal a cut-off request hop time, *cutoffRHT*, as in (7) is calculated. For every duplicate RREQ received, a reply is generated and *avgRHT* and *cutoffRHT* updated only when RREQ's RHT is below *cutoffRHT*. All destinations maintain separate *avgRHT* and *devRHT* values for sources.

$$RHT_i = \frac{(t_i - t_0)}{h_i} \tag{3}$$

$$diff_i = RHT_i - avgRHT \tag{4}$$

$$avgRHT = avgRHT + \delta \times diff_i \tag{5}$$

$$devRHT = devRHT + \mu \times (|diff_i| - devRHT) \tag{6}$$

$$cutoffRHT = avgRHT + \phi \times devRHT \tag{7}$$

Differential Evolution (DE) is used for trust value (delta and mu) optimization.

Assuming that *devRHT* approximates standard deviation of sample RHTs, by a law of large numbers in statistics, fewer than 5% of normal requests have RHTs above *cutoffRHT* calculated with $\emptyset$= 2. Next, issue that destination does not know actual value of t_0 is addressed along with local time when route discovery began.

Trust is computed by

$$\text{Trust}=\alpha^* \text{ direct trust}+\beta^* \text{ indirect trust} \tag{8}$$

In this work, parameter α and β are assigned equal weightage of 0.5.

C. Differential Evolution (DE)

Differential Evolution (DE) is a heuristic stochastic population difference based search method. DE's principle and process is similar to GA. DE algorithm has three parts: mutation, crossover, and selection. DE, unlike GA, uses difference method to realize mutation operation, which takes advantage of the colony distribution property effectively and enhances search capability. DE Difference method compensated the mutation method deficiency in GA [27]. DE is popular because of its simple principle, less parameter, and good robustness. But, basic DE depends much on parameters resulting in the algorithm leading to premature convergence. This limited extensive use of DE application. Also, the property of real DE coding has limited its application in large-scale network.

Initialization

DE starts with population of NP D-dimensional search variable vectors. Subsequent DE generations are presented by discrete time steps like t =0,1,2,…..t, t+1, etc. As vectors are likely to change over different generations to represent i^{th} population vector at current generation (i.e., at time t = t) as

$$\vec{X}_i(t) = [x_{i,1}(t), x_{i,2}(t), x_{i,3}(t)....x_{i,D}(t)] \tag{9}$$

The vectors are referred to in literature as "genomes" or "chromosomes".

Mutation Operation

Mutation operation is applied to a set of genes of all chromosomes with mutation probability *q*. Mutation operation changes/flips a gene of candidate chromosomes to avoid local optima. This is expressed for j^{th} component of each vector as

$$v_{i,j}(t+1) = x_{r1,j}(t) + F.(x_{r2,j}(t) - x_{r3,j}(t)).... \tag{10}$$

Next to increase potential population diversity a crossover scheme comes to play.

Crossover Operation

In crossover operation, all corresponding lower genes are exchanged when a chromosome's gene is exchanged for corresponding gene in another chromosome. It adds variety to the swarm. It includes two modes: index crossover mode and binomial crossover mode. The algorithm uses binomial crossover mode defined as [28]:

$$\begin{aligned} u_{i,j}(t) &= v_{i,j}(t) && if\ rand(0,1) < C_r, \\ &= xi, j(t) && else.. \end{aligned} \tag{11}$$

where C_r is a crossover factor, and *rand* is a random decimal figure between [0,1].

Selection Operation

DE involves Darwinian principle of "survival of fittest" in the selection process which is outlined as

$$\vec{X}_i(t+1) = \vec{U}_i(t) \quad if\ f(\vec{U}_i(t)) \le f(\vec{X}_i(t)), \\ = \vec{X}_i(t)\, if\ f(\vec{X}_i(t)), f(\vec{U}_i(t)),.. \tag{12}$$

where $f(\ )$ is function to be minimized. So when new trial vector yields a better value of fittest function, it replaces its target in succeeding generations. Hence, population gets better or remains constant.

IV. Results and Discussion

Proposed trust based AOMDV routing protocol is evaluated and compared with AOMDV for the network performance under wormhole attack. The simulations are carried out with 10% and 20% of the nodes being malicious. The simulations are carried for varying number of nodes in the network (25 to 125). Figs. 1-3 show Packet Delivery ratio, end to end delay, and average number of hops respectively.

TABLE II
Packet Delivery Ratio

Number of nodes	Proposed LQ CHQ AOMDV 10% malicious	Proposed LQ CHQ AOMDV 20% malicious	Proposed LQ CHQ AOMDV 10% malicious with trust	Proposed LQ CHQ AOMDV 20% malicious with trust
25	0.734	0.7051	0.858	0.8479
50	0.686	0.6656	0.8163	0.8061
75	0.6765	0.6588	0.8128	0.7892
100	0.6443	0.6313	0.7741	0.7582
125	0.6029	0.5856	0.7057	0.6966

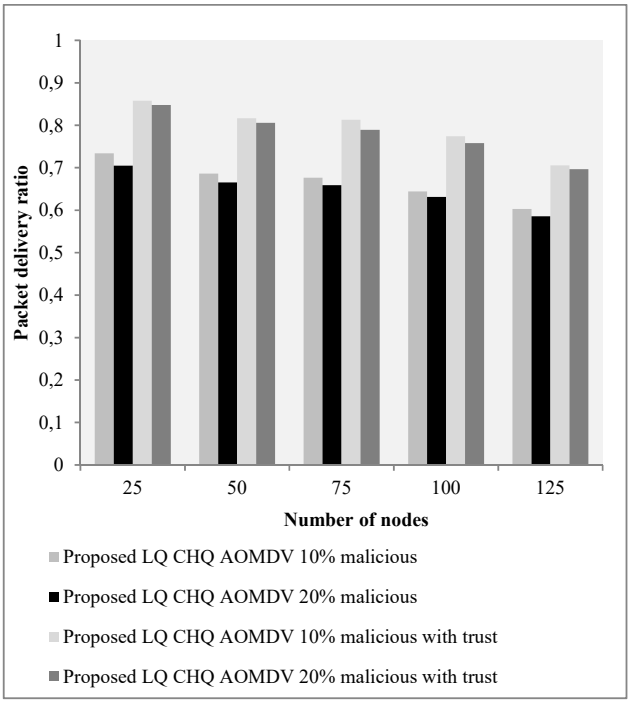

Fig. 1 Packet delivery ratio

When number of nodes is 75, the proposed method based trust with 10% of malicious nodes improved packet delivery ratio by 18.3039% when compared to proposed method without trust with 10% malicious nodes. When number of nodes is 50, the proposed method based trust with 20% of malicious nodes improved packet delivery ratio by 19.09% when compared to the proposed method without trust with 20% malicious nodes.

TABLE III
End to End Delay

Number of nodes	Proposed LQ CHQ AOMDV 10% malicious	Proposed LQ CHQ AOMDV 20% malicious	Proposed LQ CHQ AOMDV 10% malicious with trust	Proposed LQ CHQ AOMDV 20% malicious with trust
25	0.001185	0.00119	0.000788	0.000992
50	0.001578	0.001385	0.000982	0.001174
75	0.003246	0.001567	0.001185	0.002572
100	0.004802	0.001668	0.001185	0.003841
125	0.015118	0.010103	0.007155	0.011688

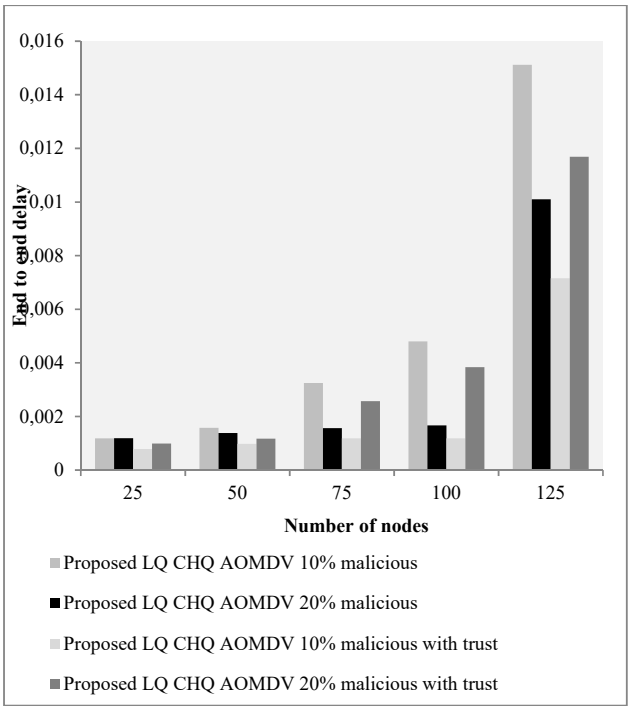

Fig. 2 End to end delay

When number of nodes is 100, the proposed method based trust with 10% of malicious nodes reduced end to end delay by 120.8285% when compared to proposed method without trust with 10% malicious nodes. When number of nodes is 500, the proposed method based trust with 20% of malicious nodes reduced end to end delay by 16.49% when compared to the proposed method without trust with 20% malicious nodes.

When number of nodes is 125, the proposed method based trust with 10% of malicious nodes decreased number of hops to sink by 33.6% when compared to proposed method without trust with 10% malicious nodes. When number of nodes is 75, the proposed method based trust with 20% of malicious nodes

decreased number of hops to sink by 23% when compared to the proposed method without trust with 20% malicious nodes.

TABLE IV
NUMBER OF HOPS TO SINK

Number of nodes	Proposed LQ CHQ AOMDV 10% malicious	Proposed LQ CHQ AOMDV 20% malicious	Proposed LQ CHQ AOMDV 10% malicious with trust	Proposed LQ CHQ AOMDV 20% malicious with trust
25	4.1	4.5	3.7	3.4
50	5.6	5.8	4.7	4.8
75	6.4	6.3	4.8	5
100	6.7	6.8	5.2	5.4
125	7.3	7.1	5.2	5.9

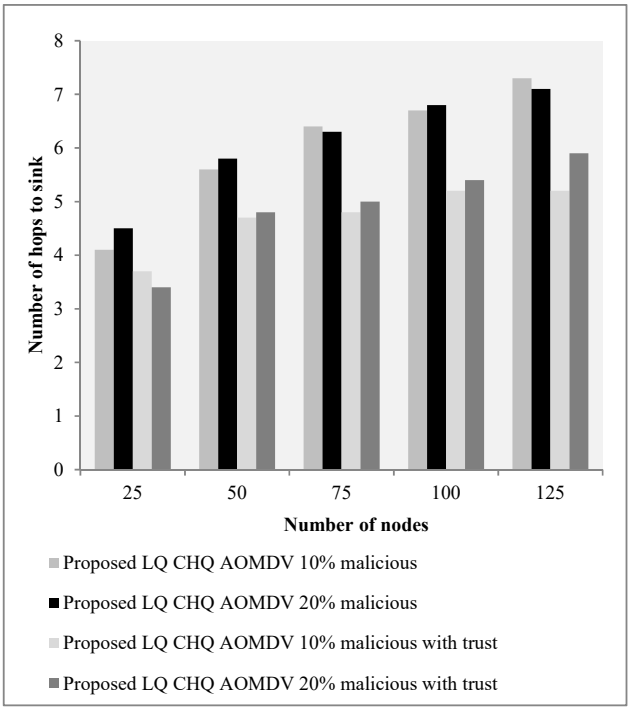

Fig. 3 Number of hops to sink

V. CONCLUSION

A self-configuring system of mobile nodes connected by wireless links is a MANET. Reputation is one entity's opinion of another. In an absolute context, it is an entity's trustworthiness. Trust, is the expectation of one entity about another's actions. Attacks on adhoc network routing protocols compromise network performance and reliability. So performance of AOMDV is improved with a trust mechanism. Differential Evolution (DE) optimizes trust value (delta and mu). Experiments were undertaken for improved AOMDV with/without trust mechanism. Results revealed that DE optimized AOMDV with trust outperformed AOMDV without trust.

REFERENCES

[1] Maheshwari, V., & Jadhav, S. Article: Survey on MANET Routing Protocol and Multipath Extension in AODV}. International Journal of Applied, 2, 1-6.
[2] Sharma, D. K., Biswash, S. K., & Kumar, C. (2010). Enhancement of Split Multipath Routing Protocol in MANET. International Journal on Computer Science and Engineering, 2(3).
[3] Qin, F., & Liu, Y. (2009). Multipath Routing forMobile Ad Hoc Network. InInternational Symposium on Information Processing.
[4] Yi, J., Adnane, A., David, S., & Parrein, B. (2010). Multipath optimized link state routing for mobile ad hoc networks. Ad Hoc Networks
[5] Mamatha, T. (2012). Network Security for MANETS. International Journal of Soft Computing and Engineering
[6] Ishrat, Z. (2011). Security issues, challenges & solution in MANET. IJCST,2(4).
[7] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: Vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.
[8] Şen, S., Clark, J. A., & Tapiador, J. E. (2010). Security Threats in Mobile Ad Hoc Networks. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, Al-Sakib Khan Pathan, Ed. Boca Raton, Florida: Taylor & Francis, 127-146.
[9] Subbaraj, S., & Sabarimuthu, P. (2014). EigenTrust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness. EURASIP Journal on Wireless Communications and Networking, 2014(1), 78.
[10] Poonam., Garg, K., & Misra, M. (2010). Trust enhanced secure multi-path dsr routing.International Journal of Computer Applications, 2(2).
[11] Somasundaram, K., & Baras, J. (2008). Path optimization techniques for trusted routing in mobile ad-hoc networks: An interplay between ordered semirings.
[12] Rashidi, R., Jamali, M. A. J., Salmasi, A., & Tati, R. (2009, October). Trust routing protocol based on congestion control in manet. In Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on (pp. 1-5). IEEE.
[13] Banerjee, A., Neogy, S., & Chowdhury, C. (2012, November). Reputation based trust management system for MANET. In Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on (pp. 376-381). IEEE.
[14] Patnaik, G. K., & Gore, M. M. (2011, March). Trustworthy Path Discovery in MANET--A Message Oriented Cross-Correlation Approach. In Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on (pp. 170-177). IEEE.
[15] Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. IET information security,4(4), 212-232.
[16] Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. Information Security, IET, 6(2), 77-83.
[17] Krishna, P. V., Saritha, V., Vedha, G., Bhiwal, A., & Chawla, A. S. (2012). Quality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks. IET communications, 6(1), 76-83.
[18] Huang, J. W., Woungang, I., Chao, H. C., Obaidat, M. S., Chi, T. Y., & Dhurandher, S. K. (2011, December). Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks. In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE (pp. 1-5). Ieee.
[19] Qu, C., Ju, L., Jia, Z., Xu, H., & Zheng, L. (2013, July). Light-Weight Trust-Based On-Demand Multipath Routing Protocol for Mobile Ad Hoc Networks. InTrust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on (pp. 42-49). IEEE.
[20] Toubiana, V., & Labiod, H. (2008, April). Towards a flexible security management solution for dynamic MANETs. In Network Operations and Management Symposium, 2008. NOMS 2008. IEEE (pp. 963-966). IEEE.
[21] Thachil, F., & Shet, K. C. (2012, September). A trust based approach for AODV protocol to mitigate black hole attack in MANET. In Computing Sciences (ICCS), 2012 International Conference on (pp. 281-285). IEEE.
[22] Jassim, H. S., Yussof, S., Kiong, T. S., Koh, S. P., & Ismail, R. (2009, December). A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network. In Communications (MICC),

2009 IEEE 9th Malaysia International Conference on (pp. 547-554). IEEE.
[23] Deepinder, E., Singh Wadhwa, E., & Tripatjot, S. P. (2011). Performance Comparison of Single and Multipath Routing Protocols in Adhoc Networks.
[24] Tamilarasan, S. M., & Eswariah, K. (2013). Link Stability With Energy Aware Ad Hoc On Demand Multipath Routing Protocol In Mobile Ad Hoc Networks. American Journal of Applied Sciences, 10(8), 844.
[25] Marina, M. K., & Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing. Wireless Communications and Mobile Computing, 6(7), 969-988.
[26] Venkatasubramanian, S., & Gopalan, N. P. (2009, November). A QoS-based robust multipath routing protocol for mobile ad hoc networks. In Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on (pp. 1-7). IEEE.
[27] Kong, S., & Chen, Z. (2010). QoS Multicast Routing Based on Double-Population Differential Evolution Algorithm. Journal of Computational Information Systems, 6(6), 1717-1725.
[28] Sharma, A., & Sinha, M. (2012). A Differential Evaluation Algorithm for routing Optimization in Mobile Ad-hoc Networks 1.

Ramya Dorai is with Prince Adhiyamaan College of Engineering, Hosur. She is currently pursuing her doctorate in India.

Rajaram. M is Vice-chancellor, Anna University, Chennai, India.