# Novel Security Mechanism to Improve QOS in MANET

P. Saravanan [1], Dr. S. Chitra [2]

[1.] Assistant Professor, Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, India
[2.] Principal, Er.Perumal Manimekalai College of Engineering, Hosur, India
saravancse@gmail.com

**Abstract:** Nodes cooperate to provide connectivity and operate without centralized administration in a Mobile Ad Hoc Network (MANET). Routing is crucial for any network as nodes transmit traffic in multihop fashion since communicating nodes might be out of range. Consequently, each node in the network not only works for itself, but must also be cooperative with other nodes. The presence of selfish nodes degrades the security and quality of service (QoS) due to its non-cooperative nature. Secure and reliable communications in MANETs due to the presences of selfish/malicious nodes, unpredictable wireless media, and host mobility is widely researched. In this paper, the concept of trust is incorporated in the routing protocol to enhance the security and QoS of the network. Managing trust in a MANET is challenging when cooperation is critical to achieving system goals. Ad hoc On Demand Distance Vector (AODV) routing protocol is enhanced with the addition of trust metrics in this study. Simulations demonstrate the effectiveness of the enhanced AODV to perform satisfactorily even in the presence of selfish nodes.
[P. Saravanan, S. Chitra. **Novel Security Mechanism to Improve QOS in MANET.** *Life Sci J* 2013;10(7s):505-509]. (ISSN: 1097-8135). http://www.lifesciencesite.com. 78

**Keywords:** Mobile Ad hoc Networks (MANETs), Ad hoc On Demand Distance Vector (AODV), Selfish Nodes, Trust

## 1. Introduction

Mobile Ad hoc Networks (MANETs) do not have centralized infrastructure, thus each node assume the role of both host and a router. Each node assists other nodes in forwarding the data packets by sharing resources like CPU cycles, bandwidth and battery power. However, some of the nodes may not cooperate and are termed as selfish nodes. Though the selfish nodes utilize the network and its services but do not consume any energy such as power or bandwidth for retransmitting the data packets of other nodes. The selfish nodes want to reserve its energy only for themselves. The presence of selfish nodes affects the reliability and performance of the network significantly [1].

Selfish nodes are not malicious nodes as it does not participate in attacks against the network. Malicious nodes are responsible for activities like alteration of traffic, fabrication of data, Denial of service (DoS) attacks and spoofing. However, selfish nodes refuse to share its resources and do not collaborate with other nodes during regular network services such as transmitting data to save their battery power [2]. The characteristics of selfish nodes [3] can be summarized as

- Non-participation in the process of routing
- Not sending Hello message and not replying Hello messages
- Dropping data packets and
- Delaying Route Request (RREQ) packet

The performance of the network is negatively affected due to selfish nodes and higher the presence of selfish nodes, greater is the degradation. Performance can be evaluated by some of the Quality of Service (Qos) parameters such as throughput, packet delivery ratio, data packets received and end to end delay [4].

The goal of the routing in MANETs is to find a route between communication nodes in an efficient manner with the topology of the network being dynamic. The Ad hoc On-demand Distance Vector (AODV) routing protocol [5] is a widely used method of routing in MANETs. AODV has many advantageous features such as loop free with quick convergence, scales well and can be incorporated into the existing protocol stack with ease. For these reasons, AODV routing is widely implemented in MANETs. In AODV routing, during the route discovery - Route Request (RREQ) messages are broadcasted from the source node to all its neighboring nodes. In turn, the neighboring nodes forward this RREQ to their neighboring nodes till the destination node or the node that contains fresh route is found. The destination node or the intermediate node with the route to destination on receipt of RREQ sends Route Reply (RREP) message to the source node and creates routing table in the forward direction [6]. The maintenance of the routes are done with the use of Hello messages. Each node in the route sends HELLO messages periodically to the neighboring nodes in the route. On the failure of the node to respond for three consecutive HELLO messages then that node is considered as failed node and RERR (Route Error) message is sent in the failed link. New

route discovery process is originated from where failure is identified. AODV routing protocol is based on the assumption that all nodes are cooperative in the coordination process; selfish nodes can easily disrupt network operations by violating protocol specification.

The concept of trust, in the network security domain, corresponds to a set of relations among nodes that participate in a protocol. Trust is a vital feature in the design and analysis of secure distribution systems. The trust relations are established on the evidence generated on the basis of the nodes previous interactions within a protocol. As a general rule, if the interactions of the node have been true to the protocol, then trust will "accumulate" between these nodes and vice-versa. The computation of the trust varies and depends on the particular protocol or application [7].

As selfish node wants to preserve its own resources while using the services of others and consuming their resources. Common way of preventing selfishness in a MANET is a detection and exclusion approach. In this paper, the focus is on the detection of selfish nodes based on trust metrics and avoiding the selfish nodes during route discovery. The traditional AODV performs its operation based on the trust values calculated for each node and decides whether the node to take part or to be avoided during routing. This trust value computed is the deciding factor about the reliability of the node for performing the routing. This trust based routing mechanism helps to identify selfish nodes in MANET and performs an efficient and effective routing. This proposed work also improves the QoS parameters like throughput and delay. The following section reviews some of the related works available in the literature, details the methodology and finally discusses the simulation results of the proposed method.

## 2. Related Work

Subramanian et al [8] proposed Trust Based Reliable AODV [TBRAODV], a trust management framework, for handling the misbehaviour problem of node and improve the performance of MANETs. To achieve reliability in routing, a trust-based system is used to track misbehaving nodes, and isolate them from routing. The proposed TBRAODV protocol implements a trust value for each node in the network. The trust was calculated on the basis of successful transmission or failure to transmit of RREQ, RREP and the amount of data transmitted by the node. Based on the trust value nodes are either allowed to participate in routing or identified as misbehaving node. The proposed scheme enhances reliability in AODV routing and results in better QoS in the form of higher PDR, decreased delay and improved throughput. Simulation results demonstrate that the proposed protocol provides more consistent and reliable data transfer compared with general AODV when misbehaving nodes are part of the network.

Bakar et al [9] proposed a method through direct and indirect approach for trust value computation among anonymous nodes. To evaluate trust values the parameters like reputation, knowledge, observation and context were used. The trust schema that is build is used to allow the resource to be shared among trusted nodes. Cho et al [10] provided a detailed discussion on the concepts and properties of trust. A survey of trust management available for MANETs and accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs was discussed and analyzed.

Manoj et al [11] addressed the security issues raised by misbehaving entities in MANETs by including trust and certification authority in the routing. Trust is allocated to every node based on the available energy and the nodes are clocked, and time lined. The nodes are monitored by a Centralized system and ensure that the certificate exchange is done only to trusted nodes, and the malicious nodes are excluded. The data exchange is protected as the certificate authority allows only the trusted nodes to participate in the network, isolating the malicious nodes. Certificate authority employs fuzzy based analyzer to discriminate between trusted and malicious behavior of nodes. The proposed method is more secure, reliable and assists in improving the security in military operations.

Saravanan et al [12] provided an implementation of trust worthy architecture. Implementation provides trusted services, as well as protection of confidential information, secures communication, secures routing protocol usage, secured mobility model, reliable communication and provides optimum quality of service metrics for the mobile ad hoc networks. Gong et al [13] proposed to use trust vector model in routing protocols. Each node is assigned trust vector parameters which is evaluates the neighbors through monitoring neighbors' pattern of traffic in the network. The proposed trust vector model was integrated into Dynamic Source Routing (DSR) and AODV. The performance was evaluated by comparing the simulation results of with and without the proposed trust method. Results validate that modified routing protocols are effective for detecting malicious nodes and mitigate their attacks.

## 3. Material and Methods

Due to the distinctive characteristics of MANET environments and the intrinsic unreliability of the wireless channel, the concept of trust in MANETs is different. The main property of trust in MANET environments is that trust is dynamic, not static. Trust establishment in MANETs should be

based on temporally and spatially local information: due to node mobility or failure, information is typically incomplete and can change rapidly [14]. To capture the dynamicity of trust, trust should be expressed as a continuous variable, rather than as a binary or even discrete-valued entity [15]. In MANET environments, trust is subjective [16]; a trustor node may determine a different level of trust against the same trustee node due to different experiences with the node derived from a dynamically changing network topology. Trust is not necessarily transitive such as if A trusts B, and B trusts C, it does not guarantee A trusts C [10].

The metric of trust used in this study is based on two parameters. First, trust is computed on the probability of the lost data packets and the second parameter based on the monitoring of the neighboring nodes. The difference in number of sent packets and received packets can be easily computed. The differences are caused by loss of packets. The possibility of packets being lost can be computed as follows

$$P_l = \frac{P_{diff}}{P_{sent}}$$

where $P_{diff}$ is obtained by computing the difference between the number of data packets sent and received. Trust can be computed as the difference in number of sent and received packets not occurring at time S.

$$T_{pl} = \left(1 - P_l(s)\right)$$

The trust that node A has on B can be computed as follows:

$$T_{a,b} = \delta_1 T_s^b + \delta_2 T_o^b$$

where $\delta_1$ and $\delta_2$ are weight factors such that $\delta_1 + \delta_2 = 1$; $T_s^b$ is the node A valuation of node B based on direct monitoring of node B and $T_o^b$ is the weighted sum of the other nodes trust on node B. Varying the weight factors to give more weightage for self-assessment or for the assessment of other nodes. The computation for the $T_s^b$ and $T_o^b$ are as follows:

Node A computes $T_s^b$ by directly monitoring B,

$$T_s^b = f(\alpha)$$

where α is the traffic statistic which is given by $\alpha = f(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ ; $\alpha_1$ is the total packets dropped by node B, $\alpha_2$ packets dropped by B due to congestion, $\alpha_3$ Node A's assessment of B's priority to B's self-packets vs. all other nodes' packets, $\alpha_4$ packet forwarding delay by B.

$T_o^b$ is the trust computed by set of other nodes O on node B.

$$T_o^b = \frac{\sum_{i \in O} \left(T_{i,b} * T_{a,i}\right)}{|O|}$$

Thus, the trust metric for the node is computed as

$$T = T_{pl} + T_{a,b}$$

In this study, the concept of trust takes into account of the packets lost as selfish nodes tend to drop data packets and trust based on monitoring the nodes. Trust represents the degree to which a node is reliable during any interaction with the node. The extent of this trust is measured by a continuous real number, and is denoted as the trust value *T*. During the nodes' communications, only when a node is trustworthy enough for another node and satisfies the trust requirement can it participate in the communication initiated by that node.

## 4. Results and Discussion

Simulations are performed in MANET designed with 15 nodes for the following scenarios:

- MANET without selfish nodes with AODV
- MANET with 20 % of selfish nodes and AODV
- MANET with 20 % of selfish nodes and Proposed trust AODV

The nodes transmit CBR traffic, the performance of AODV routing protocol and the proposed trust AODV are evaluated on the basis of throughput, cache replies used and end to end delay. The experiments setup is given in table 1.

Table 1: simulation parameters

| | |
|---|---|
| Simulation area | 2 sq km |
| Number of nodes | 15 |
| % of nodes which are malicious | 20 |
| Bandwidth | 2 Mbps |
| Traffic | Constant Bit Rate |
| Transmission power of node | 0.005W |

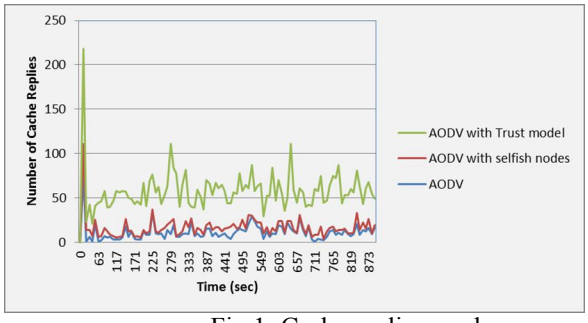


Fig 1: Cache replies used

To improve the routing protocols route caching concept are used. Cache memory is a small, temporary memory used to store the recently accessed data values. In MANET, cache memories are used to store the routes that were used recently. Route caching helps decrease the flooding of network and latency. Decrease in the flooding, decreases the overhead in route discovery process. So Route caching will increase the performance of routing protocols. Figure 1 shows that the presence of selfish nodes increase the cache replies used. The proposed routing has maximum cache replies.

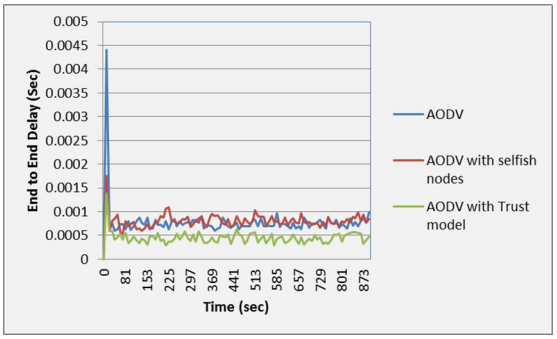


Fig 2: End to End Delay

Figure 2 shows the end to end delay for different scenarios, it is observed that the proposed routing has significantly lower end to end delay when compared to traditional AODV (with or without selfish nodes in network). As the routes to the destination are made of trustworthy nodes, the end to end delay is considerably reduced in the proposed trust AODV routing.

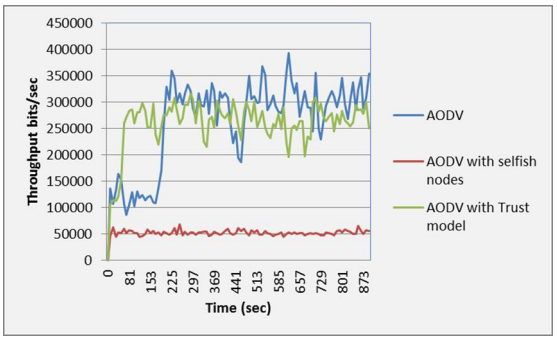


Fig 3: Throughput in bits per second

Figure 3 shows the throughput in bits per second, it is observed that without the presence of selfish nodes average throughput is around 2,62,000 bits per second. But in the presence of 20 % of the selfish nodes the throughput approximately reaches to 51,000 bits per second. Throughput is 5 times lower in the presence of 20% of selfish nodes. On using trust in the routing, the throughput is around 2,58,000 bits/sec. Though, the cache replies used is higher for the proposed routing, the end to end delay is less and significant improvement in the throughput is achieved by the proposed trust routing.

## 5. Conclusions

Most security approaches proposed for MANETs are designed upon the fundamental assumptions of the trustworthiness of the participating nodes and the underlying networking system. The characteristic freedom in MANETs introduces challenges for trust management, principally when nodes do not have any former knowledge of each other. In this paper, we focus on the detection of selfish nodes based on trust metrics and avoid the selfish nodes during route discovery. The simulation results show a good improvement of parameters for the proposed trust routing than the exiting approach. The traditional AODV is affected due to the existence of selfish nodes, which results in low throughput and also causes the delay to increase. The proposed protocol has shown improved QoS parameters values where trust values are used to identify the selfish nodes in the route ting. This approach of the proposed protocol has resulted in increased throughput and decreased delay involved in routing.

## References

1. Dipali Koshti, Supriya Kamoji, Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011.
2. Shailender Gupta, C. K. Nagpal and Charu Singla, Impact of Selfish Node Concentration in Manets, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011
3. S. Marti, T. J. Giuli, K. Lai, M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. of MobiCom 2000, Boston, August 2000.
4. Mr. Amir Khusru Akhtar & G. Sahoo Mathematical Model for the Detection of Selfish Nodes in MANETs, International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 2231 –5292, Volume-1, Issue-3.
5. Charles E. Perkins and Elizabeth M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In Charles E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000
6. Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma, Performance analysis of AODV, DSR & TORA Routing Protocols, IACSIT International Journal of

Engineering and Technology, Vol.2, No.2, April 2010.
7. Theodorakopoulos, G., & Baras, J. S. (2006). On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 24(2).
8. Subramanian, S., & Ramachandran, B. (2012). Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks. arXiv preprint arXiv:1202.1664.
9. Bakar, A. A., Ismail, R., Jais, J., & Manan, J. (2009, January). Forming Trust in Mobile Ad Hoc Network. In Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on (Vol. 3, pp. 470-474). IEEE.
10. Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 13(4), 562-583.
11. Manoj, V., Aaqib, M., Raghavendiran, N., & Vijayan, R. (2012). A Novel Security Framework Using Trust And Fuzzy Logic In Manet. International Journal, 3.
12. Saravanan, D., Chandrasekaran, R. M., Prabha, B. V., & Dhulipala, V. S. (2011). Trust Worthy Architecture Implementation for Mobile Ad hoc Networks. International Journal on Computer Science and Engineering, 3(7), 2601-2609.
13. Gong, W., You, Z., Chen, D., Zhao, X., Gu, M., & Lam, K. Y. (2010). Trust based routing for misbehavior detection in ad hoc networks. Journal of Networks, 5(5), 551-558.
14. L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.
15. W. J. Adams, G. C. Hadjichristofi and N. J. Davis, "Calculating a Node's Reputation in a Mobile Ad Hoc Network," Proc. 24th IEEE Int'l Performance Computing and Communications Conference, Phoenix, AX, 7-9 April 2005, pp. 303-307.
16. Abdul-Rahman and S. Hailes, "Using Recommendations for Managing Trust in Distributed Systems," Proc. IEEE Malaysia Int'l Conf. on Communication, Kuala Lumpur, Malaysia, Aug. 1997.

1/8/2013