

# Enhanced dynamic source routing for verifying trust in mobile ad hoc network for secure routing

Salman Ali Syed, Shahzad Ali

Department of Computer Science, College of Science and Arts, Jouf University, Tabarjal, Kingdom of Saudi Arabia

---

## Article Info

### Article history:

Received Jan 6, 2021

Revised Jul 13, 2021

Accepted Jul 30, 2021

---

### Keywords:

DSR

MANET

Routing

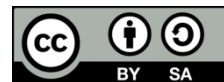
Trust

---

## ABSTRACT

Secure data transfer in mobile ad hoc network (MANET) against malicious attacks is of immense importance. In this paper, we propose a new enhanced trust model for securing the MANET using trust-based scheme that uses both blind trust and referential trust. In order to do this, the trust relationship function has to be integrated with the dynamic source routing (DSR) protocol for making the protocol more secure. We thoroughly analyze the DSR protocol and generate the performance matrices for the data pertaining to packets sent, packets received, packets loss, and throughput. We also analyze the outcome attained from the improvised trust establishment scheme by using the three algorithm implementations in NS2 simulator for detecting and preventing various types of attacks.

*This is an open access article under the [CC BY-SA](#) license.*



---

### Corresponding Author:

Salman Ali Syed

Department of Computer Science, College of Science and Arts, Jouf University

Aljouf province, Tabarjal, Kingdom of Saudi Arabia

Email: drsalman1232@gmail.com

---

## 1. INTRODUCTION

Ad hoc networks are the kind of network that does not have the support of fixed infrastructure. Mobile ad hoc network (MANET) features mobile nodes that work in a decentralized manner without any support from fixed infrastructure. MANET comprises many applications that tend to provide real life situations [1]. In most of the situations, MANET are precisely used to conduct meetings or communication processes among distinct groups outside offices using Bluetooth [2] or similar technologies based on ad hoc communications [3]. Routing is one of the challenging tasks in a MANET due to challenges associated with mobility of nodes, network bandwidth, and scarce energy resources [4]-[10]. It is desired to design an efficient and adaptable routing protocol that can efficiently handle the dynamic network conditions. On the other hand, routing protocols must be capable of supporting different types of services to distinct applications that makes use of MANET [11], [12] which is dynamic and more flexible in adapting network topology that makes a MANET prone to security attacks in large scale environment. Nodes will communicate with each other for transmitting the controlling the data packets by obtaining the trust among nodes to secure the network [13], [14]. Conventionally speaking MANET has many features than that of conventional wireless networks and similarly trust of wired network is also not feasible for MANET due to which we make use of trusted third party for verifying and authenticating nodes [15].

In MANET, nodes must evaluate trust locally by themselves as to secure the data. A routing protocol should be designed which is capable of identifying a secure path among various cooperating nodes by validating the transitional nodes and validating the reliability of the path [16]. Almost all the secure routing protocols are exposed to attacks like packet dropping and flooding and more over the existing protocols as they are not intended to guarantee the inclination of a network [17], [18]. While a limited trust

models have been intended for performing secure routing but none of them can handle all the possibilities and this area is open for research.

In this paper, we have proposed a trust based security model aimed to implement secure routing in a MANET which is capable for characterizing devices based on many aspects in a heterogeneous environment that depends on the residual battery power [19]. Hence evaluating the trust within a MANET is considerably a challenging task that incorporates distinct network capabilities that are further matched with the traditional infrastructure governed networks [20]. It is obligatory that each node in a MANET must be assessed by its own trust first then the trust of other nodes that are within the range [21]. The available trust models are designed for static networks making them unapplicable in the MANET. There is a need for designing novel trust models for MANETs [22].

In this paper, we propose an estimation-based trust model that is based on each node's trust level attained in the trust matrix evaluated for each node that is available in MANET. The proposed mechanism will further deploy and implement intangible scenarios highlighted, i) trustiness is defined for each node in a trust model by evaluating trust lever using a function (that comprises of blind and referential trust methods) [23], ii) the attached trust model is enhanced with dynamic source routing (DSR) protocol [24], iii) then the protocol is assessed by evaluating by using extensive simulations performed in NS2 simulator [25].

## 2. THE PROPOSED ALGORITHM

The association identified between two or more nodes that perform any activity, is merely considered to be Trust or Trust model. This definition differs based on many of the criteria though it comprises of these main terms: i) trustor, ii) trustee, iii) referential, where Trustor is the main role-based node which evaluates the trust level and then Trustee is the node whose trust level is acquired and finally referential node is the one who provides recommendations about any specific node.

### Algorithm: Blind Trust-based trust calculation

```

Step 1: Start
Step 2: suppose N1 finds N2 to be trustee from trust table then, N1 will send a packet to N2
Step 3: number_of_packets= number_of_packets + 1
Step 4: if N1 verifies that N2 has forwarded packet successfully, then increment
No_of_Packets_forwarded
Step 5: else decrement No_of_Packets_forwarded
Step 6: evaluate trust level of N2 and update in trust table
Step 7: Stop

```

### Algorithm: Referential Trust based trust calculation

```

Step 1: Start
Step 2: calculate the number of hops between node N1 and Trustee node N2 using equation 3
Step 3: assign the resultant to trust value, if no value received then set to 0
Step 4: Stop.

```

### Algorithm: Trust evaluation for implementing secure routing based on trust in MANET

```

Step 1: Start
Step 2: Root node broadcasts RERQ for root discovery to neighbor nodes Ni
Step 3: Ni node verifies its own trust evaluation matrix for threshold value
Step 4: if trust evaluated is greater than 0 then it broadcasts to its own neighbors
Step 5: if any neighbor node responds then go to step 7
Step 6: go to step 3 until target node is reached
Step 7: root node checks the neighboring nodes and selects the shortest or fastest route
Step 8: root node transmits the data packets in the evaluated root
Step 9: Target nodes sends conformation message
Step 10: if conformation message is received from target node in the time span then rest of
the packets will be sent in the root.
Step 11: if conformation message not received in time, update trust matrix and go to step 7
Step 12: if malicious behavior is detected by the root node then trust matrix is updated
to -1 and go to step 7
Step 13: Stop

```

## 3. RESEARCH METHOD

To acquire the trust, we need secure topology information that is attained by micro devices considered to be nodes which communicate with one another in a fully authenticated distributed environment using micro sensors. The process comprises of following:

- Quantifying trust: it refers to the degree of trust that is estimated for a node in the range of -1 to +1 where -1 denotes distrust and +1 denotes trust-oriented node and these are the two extreme values.

- Computing Trust: the computation of trust between trustee node and trustor node is implemented in two aspects a) Blind Trust and b) Referential Trust, where Blind trust the aspect which does not take any consideration of referential trust aspects and is purely based on previous experience trust is evaluated, which may be positive or negative based on previous experiences or priorities and is evaluated as (1), Similarly, trust is evaluated based on the earlier statistics upon a trustee node for a node  $N_0$  or a root node is (2):

$$Y = \tanh(x) \quad (1)$$

$$N_0 = \tanh \sum_{i=1}^n (U_i W_i P_i) \quad (2)$$

where  $P_i$  denotes total number of experiences of trust node  $i$  based on the communication which took earlier,  $W_i$  denotes the weights attained from experience that is whether the node is in blacklisted or not or is it under malicious list or not and  $U_i$  denotes the trust value in the range of -1 to +1 which is obtained from the recommendation or reputation levels of a trust. When trust estimator wants to utilize the third-party node (TP) for obtaining trust which has a good trust value is denoted as (3):

$$\text{ThirdParty}_T = \frac{1}{n} \sum_{i=1}^n (B_T V_i) \quad (3)$$

where  $B_T$  is the direct trust attained and  $V_i$  is the trust of third-party node.

- Making decision based on trust value: for maintaining the security level we need a threshold value that changes based on environment being evaluated which requires huge aspect of decision making, which is done with the (4) where if the DecisionT value is evaluated to  $>0$  then it is trusted otherwise not trusted.

$$\text{Decision}_T = V - T_{\text{threshold}} \quad (4)$$

- Trust Information Table: we need to create and maintain the trust information table which comprises of all the previous entries of the trust being evaluated for further reference with attributes such as id, trust level, and evaluated on.

#### 4. RESULTS AND DISCUSSION

We have implemented all the algorithms in NS2 simulator with maximum simulation time of 500 sec over 50 mobile nodes with a transmission range of 250 meters and topology used is 1000x1000 meters with DSR routing protocol at a maximum bandwidth of 1 Mbps using constant bit rate (CBR) traffic with a packet size of 512 and with 5 malicious nodes with a threshold of 0.60. Table 1 denotes the simulation data attained by taking average of 20 samples which we have compared with the standard DSR protocol and compared it with malicious node too. We have considered various aspects such as flooding of packets, packet dropping by nodes, performance comparisons and the performance matrix is generated and clearly defined in the table by evaluating the ratio.

**Table 1. Simulation data attained by taking packet delivery ratio and throughput, average of 20 samples**

Interaction between Nodes		Delivery of packet (Ratio)		Attained throughput	
Initial Node	Subsequent Hop	Standard DSR	With Proposed algorithm	Standard DSR	With Proposed algorithm
Root Node $N_0$	$N_1$	4.5	20.56	5.3	5.96
	$N_2$	28.3	47.36	6.4	7.35
	$N_3$	45.87	88.42	4.98	5.69
	$N_4$	4.2	18.98	7.42	8.25
	$N_5$	21.63	45.54	6.35	6.92
	$N_6$	41.35	92.57	4.12	5.37

Table 2 denotes the simulation data attained by taking average of 20 samples which we have compared with the standard DSR protocol and compared it with malicious node too. We have considered two aspects that is packet received and the percentage of packet loss and the performance matrix is generated and clearly defined in the table by evaluating the ratio. Figure 1 represents the RouteRequest (RREQ) root node broadcast for transmitting and receiving the data from  $N_0$  to other nodes with varying mobility speeds with a minimum of 5 m/s and a pause time of 0, hence it is clear from the figure that the proposed algorithm performs better than DSR. Figure 2 shows that the graph attained using total RREQ that is sent and received

from node  $N_0$  with the rest of the nodes with the traversal speed of 5 m/s with 0 pause time and it is evident from the figure that the proposed method is better as compared to the existing DSR protocol.

Figure 3 shows that the graph attained using total RREQ that is the packet lost when sent and received from node  $N_0$  with the rest of the nodes with the traversal speed of 5 m/s with 0 pause time and it is very clear that the proposed method is better than DSR protocol. The throughput in Figure 4 is attained by considering various criteria such as packet loss and malicious nodes and it is observed that the achieved packet delivery ratio is lesser for the existing DSR method as compared to the proposed method. From the four figures we can say that the enhanced methodology is capable of securing the routing process for estimating the trust model.

Table 2. Simulation data attained for packets received and lost by taking average of 20 samples

Interaction between Nodes		Packet Sent	Packet Received		Packet Loss (%)	
Initial Node	Subsequent Hop		Standard DSR	With proposed algorithm	Standard DSR	With proposed algorithm
Root Node $N_0$	N1	600	25.26	120.54	98.25	72.65
	N2	650	160.52	336.85	73.65	51.24
	N3	700	350.95	625.35	54.28	15.27
	N4	750	28.69	148.62	98.74	72.41
	N5	800	205.82	425.32	42.32	55.67
	N6	850	342.89	720.56	54.13	12.12

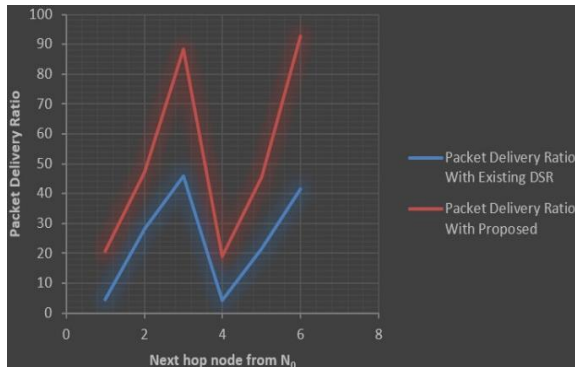


Figure 1. Packet delivery ratio with existing DSR and proposed method

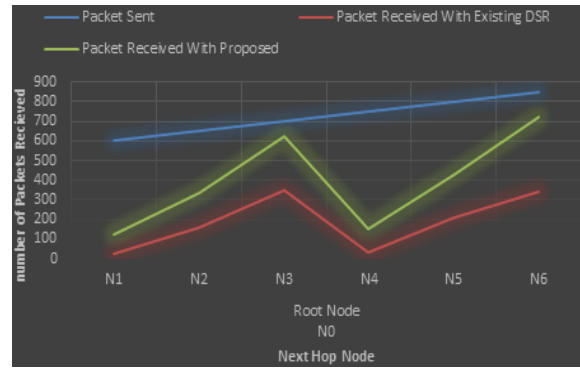


Figure 2. Packets sent and received with existing DSR and proposed method using RREQ

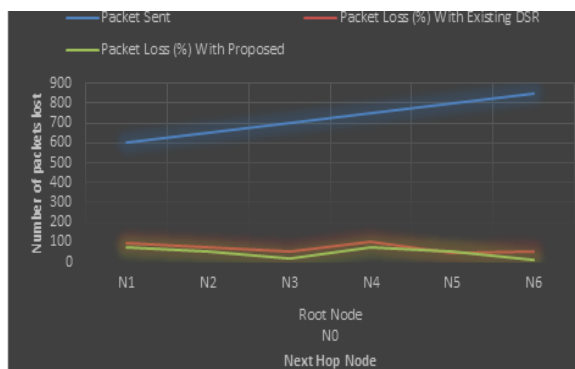


Figure 3. Packets lost with existing DSR and proposed method using RREQ

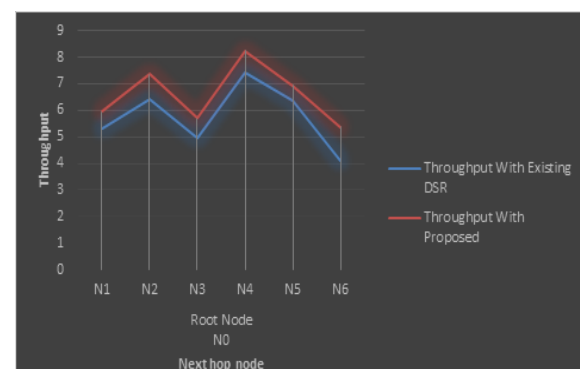


Figure 4. Throughput with existing DSR and proposed method

### 5. CONCLUSION





In this paper, we proposed a new enhanced trust model, which secures the MANET where the trust-based scheme is specified using the trust relationship function as the trust is evaluated using both blind trust and referential trust. We have integrated the trust relationship function with the standard DSR protocol. The

new enhanced protocol secures the protocol and yields improved performance in terms of multiple performance metrics. The performance of the existing DSR protocol and the proposed protocol is evaluated using extensive simulations in NS2 simulator. By analyzing the performance, we can conclude that the proposed mechanism with an improved trust establishment scheme outperforms the standard DSR protocol. Three algorithm implementations in NS2 simulator were done for detecting and preventing various types of attacks. The efficiency of the proposed model is clearly illustrated in the results attained. For the future work, we aim to adapt the proposed trust model for various other routing protocols for providing better security solutions for MANETs.





## REFERENCES

- [1] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Transaction on Mobile Computing*, vol. 11, no. 9, pp. 1514-1531, 2012, doi: 10.1109/TMC.2011.160.
- [2] A. Banerjee, S. Neogy, and C. Chowdhury, "Reputation based trust management system for MANET," *2012 Third International Conference on Emerging Applications of Information Technology*, 2012, pp. 376-381, doi: 10.1109/EAIT.2012.6407975.
- [3] F. Bao, R. Chen, M. Chang, and J. H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169-183, 2012, doi: 10.1109/TCOMM.2012.031912.110179.
- [4] K. Z. Bijon, M. M. Haque, and R. Hasan, "A trust-based Information sharing model (TRUISM) in MANET in the presence of uncertainty," *2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, 2014, pp. 347-354, doi: 10.1109/PST.2014.6890959.
- [5] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Transaction on Wireless Communications*, vol. 10, no. 9, pp. 3064-3073, 2011, doi: 10.1109/TWC.2011.071411.102123.
- [6] B. K. Chaurasia and R. S. Tomar, "Trust management model for wireless ad hoc networks," *Proceedings of the international conference on soft computing for problem solving (SocProS 2011)*, vol. 130, 2012, pp. 201-206, doi: 10.1007/978-81-322-0487-9\_20.
- [7] I. R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Integrated social and quality of service trust management of mobile groups in ad hoc networks," *2013 9th International Conference on Information, Communications and Signal Processing*, 2013, pp. 1-5, doi: 10.1109/ICICS.2013.6782950.
- [8] R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization," *Ad Hoc Networks*, vol. 19, pp. 59-74, 2014, doi: 10.1016/j.adhoc.2014.02.005.
- [9] F. De Rango, F. Guerriero, and P. Fazio, "Link-stability and energy aware routing protocol in distributed wireless networks," *IEEE Transaction on Parallel Distributed Systems*, vol. 23, no. 4, pp. 713-726, 2012, doi: 10.1109/TPDS.2010.160.
- [10] M. K. Denko, T. Sun, and I. Woungang, "Trust management in ubiquitous computing: a Bayesian approach," *Computer Communications*, vol. 34, no. 3, pp. 398-406, 2011, doi: 10.1016/j.comcom.2010.01.023.
- [11] M. Gunasekaran and K. Premalatha, "TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks," *IET Information Security*, vol. 7, no. 3, pp. 203-211, 2013, doi: 10.1049/iet-ifs.2012.0141.
- [12] I. Jawhar, Z. Trabelsi, and J. Al-Jaroodi, "Towards more reliable and secure source routing in mobile ad hoc and sensor networks," *Telecommunication System*, vol. 55, no. 1, pp. 81-91, 2014, doi: 10.1007/s11235-013-9753-7.
- [13] K. Ullah, R. Das, P. Das, and A. Roy, "Trusted and secured routing in MANET: An improved approach," *2015 International Symposium on Advanced Computing and Communication (ISACC)*, 2015, pp. 297-302, doi: 10.1109/ISACC.2015.7377359.
- [14] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transaction on Information Forensics and Security*, vol. 8, no. 6, pp. 924-935, 2013, doi: 10.1109/TIFS.2013.2240299.
- [15] S. Mutlu and G. Yilmaz, "Simulation and performance analysis of distributed cooperative trust based intrusion detection framework for MANETs," *Journal of Aeronautics and Space Technologies*, vol. 6, no. 2, pp. 49-57, 2013.
- [16] D. G. Patel, P. A. Pandey, and M. C. Patel, "Trust based routing in ad-hoc networks," *International Journal of Current Engineering Technology*, vol. 4, pp. 860-863, 2014.
- [17] M. Saadoune, A. Hajami, and H. Allali, "Distance's quantification algorithm in AODV protocol," *International Journal of Computer Science Information Technology*, vol. 6, no. 6, pp. 177-188, 2014, doi: 10.5121/csit.2014.41117.
- [18] A. M. Shabut, K. Dahal, Bista, and I. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101-2115, 2015, doi: 10.1109/TMC.2014.2374154.
- [19] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET," *Ad Hoc Networks*, vol. 30, pp. 84-98, 2015, doi: 10.1016/j.adhoc.2015.03.004.
- [20] G. Thanigaivel, N. A. Kumar, and P. Yogesh, "TRUNCMAN: Trust-based routing mechanism using non-cooperative movement in mobile ad-hoc network," *2012 Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 2012, pp. 261-266, doi: 10.1109/DICTAP.2012.6215430.
- [21] P. B. Velloso, R. P. Laufer, D. D. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172-185, 2010, doi: 10.1109/TNSM.2010.1009.19P0339.
- [22] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc Networks with trust management using uncertain reasoning," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4647-4658, 2014, doi: 10.1109/TVT.2014.2313865.
- [23] Z. Yan and M. Wang, "Protect pervasive social networking based on two-dimensional trust levels," *IEEE Systems Journal*, vol. 11, no. 1, pp. 207-218, 2014, doi: 10.1109/JSYST.2014.2347259.
- [24] H. Zhao, X. Yang, and X. Li, "cTrust: trust management in cyclic mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2792-2806, 2013, doi: 10.1109/TVT.2012.2230411.
- [25] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 22-32, 2014, doi: 10.1109/TPDS.2013.36.

**BIOGRAPHIES OF AUTHORS**

**Salman Ali Syed**     working as an Assistant professor in Department of Computer Science, Jouf University, Kingdom of Saudi Arabia. He completed his Ph.D. from Pacific academy of Higher Education and Research University, Udaipur, India. He completed his master's degree from University College of Engineering, JNTU Anantapur and bachelor's degree from Jawaharlal Nehru Technological University, Hyderabad. His research areas include MANETs, Databases, Network Security, and Data Mining. He can be contacted at email: drsalman1232@gmail.com.



**Shahzad Ali**     received his M.Sc. in Telematics Engineering in 2011 and his Ph.D. in Telematics Engineering from University Carlos III of Madrid, Spain in 2014. Currently, he is working as assistant professor at department of Computer Science, Jouf University, Tabarjal, Saudi Arabia. His research interests include performance analysis of context-aware applications, wireless sensor networks, vehicular ad hoc networks, and opportunistic networks. He has published his research work in top conferences like INFOCOM and Mobihoc. and well-reputed journals of his field. He is also acting as a reviewer of many well-reputed journals and also acting as TPC for many well-known conferences. He can be contacted at email: malikshahzadali@gmail.com.