International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5441-5446


# Design and Implementation of Trust-based Secure Routing Protocol for MANETs

**Mukesh Kumar Garg**[1]
*Department of Computer Engineering,*
*YMCA University of Science & Technology,*
*Faridabad, Haryana, India.*

*Orcid Id: 0000-0002-2863-4019*

**Neeta Singh**[2]
*Department of Computer Science and Engineering,*
*School of ICT, Gautam Buddha University,*
*Greater Noida, Uttar Pradesh, India.*

**Meena Rao**[3]
*Department of Electronics and Communication Engineering,*
*Maharaja Surajmal Institute of Technology,*
*C-4, Janakpuri, New Delhi, India.*

**Abstract**

A mobile ad hoc network (MANET) consists of independent nodes wherein the system has to work without any set infrastructure in place. Network performance depends upon efficient transmission of packets between nodes. However, dynamic nature of nodes makes secure transmission of packets difficult. In this paper, a Trust-based Secure Routing Protocol for MANETs (TBSRPM) has been proposed in order to transmit packets efficiently with the help of a trust-based communication feature. TBSRPM establishes a secure route between source and destination without any intruders or malicious nodes. TBSRPM depends on the trust of any node on its neighbor node. Here trust mechanism is used as a substitute to techniques like cryptography. Trust value (TV) and level of trust (LOT) is assigned to the information flow, which decides what level of encryption (security action) is required to the current routing information at a source node. Hence, routing information is encrypted based on the TV. The proposed TBSRPM takes into consideration both node trust (NT) and route trust (RT), respectively. To validate the protocol, test cases have been shown.

**Keywords:** MANET; TBSRPM; TV; LOT; NT; RT

## INTRODUCTION

A fundamental characteristic of MANET is that they are able to configure themselves on-the-fly without the involvement of a centralized administrator or any pre-existing infrastructure. Every mobile node in a network is autonomous. A common assumption about the routing protocols that all nodes are trustworthy and cooperative. To enhance security in MANETs, it is important to evaluate the trustworthiness of nodes without any centralized or monitoring authority. Also, the major issues that concerns MANETs and its proper functioning are: Trust-based routing and Security. These issues are directly related to efficient delivery of packets and how effective the network is. Trust is the degree of belief about the future behaviour of other entities or nodes. Behaviour of nodes or entities is determined on the basis of its previous history. In MANETs, trust can be divided into two categories i.e. i) Node Trust (NT) and ii) Route Trust (RT). The various mathematical models have been used for calculating Trust Value (TV). Based on the Level of Trust (LOT), the nodes can communicate with its neighbor. In the proposed protocol, RT plays an equal role as NT. Here, network security enhancement is completely performed by taking into consideration TV.

The remainder of this paper is organized as follows. Section II provides a brief overview of related research work. Section III describes details incorporating trust into the node. The design of experiment and results are presented in Section IV. Finally, in Section V we present our conclusions and perspective for future work.

## RELATED RESEARCH WORK

The implementation as well as performance metrics of an ad hoc network is solely dependent upon the cooperative and trusting nature of its nodes. Trust and security are two concepts which are interdependent on each other. For example, cryptographic techniques are used for improving security in MANETs. However, this technique is highly dependent on trusted key exchange and trusted key exchange cannot take place without requisite security services in place. So, both the entities, trust as well as security, are interdependent. It is because of the inter-reliance that either of these terms are used when defining a secure system. The routing protocols for MANETs incorporating security mechanisms have been discussed by various authors. Garg et al. describe the routing and security issues for trust based framework in MANETs [1]. The relative performance analysis of reactive or on-demand routing protocol is described by Garg et al [2]. Here, the authors simulate and describe the behavior of reactive routing protocols and it is shown that they consume less bandwidth as compared to table driven routing protocols. The most popular reactive routing protocol Ad Hoc On-Demand Distance Vector (AODV) Routing was first proposed by Perkins and Royer in the year 1999 [3]. Also, for secure transmissions and routing using AODV hash chains and digital signatures were also used [4]. However, the issue of route

dependability is not discussed. Yan et al. have presented a trust evaluation based security solution that tries to provide effective data protection while routing [5]. The authors have shown through suitable results that the decision related to secure route selection or other security related issues should be based on trust analysis and evaluation among network nodes. Clarity on the trust relationship makes it easier to take appropriate security measures. Also, a general trust based communication is further introduced in literature [6]. Here a node or an entity assigns trust to other nodes based on the previous transactions. Trust information is gathered based on the information gathered by one node about other node in passive state. Moreover, the framework is established without any central trust authority. However, the authors have not extended the model to traditional routing protocol like AODV and have not analyzed issues like malicious behavior as well as security against attacks. A Trusted AODV (TAODV) that employs the idea of a trust to protect routing behaviour in the network layer of MANETs has also been proposed in literature [7]. A routing protocol that is based on securing the routing information from unauthorized users is further discussed by Nekkanti et al. [8]. A trust based framework to improve the security and robustness of ad hoc network routing protocols is further implemented by Meka et al. here, a source node selects more trusted paths instead of shorter ones while routing. AODV routing scheme is used for simulating the model [9]. However handling of malicious nodes as well as security schemes are not discussed in the paper. In another technique presented in literature the trust estimation between nodes in ad hoc network based on the QoS parameters is used to update trust [10]. In [11] a new authentication service and trust level is attached in every packet to make the routing in MANETs secure. Mangrulkar et al. proposed an algorithm that has an additional field to store TV in the request packet to indicate node trust on neighbor [12]. Depending on level of trust factor, the routing information is then based on the highest TV value among all nodes. An algorithm based on the concept of honest value, that in turn is calculated on the concept of hop and trust, has also been presented in literature to protect the network from malicious nodes [13]. At present secure routing is still an open research question and needs further discussion.

## TRUST-BASED SECURE ROUTING PROTOCOL (TBSRP)

In TBSRP, the packet consists of control information along with real information. The format of data packet header is shown in Fig.1.

| P_Type | P_id | S_add | D_add | TTL | LVN | TV |
|---|---|---|---|---|---|---|

**Figure 1.** Format of data packet.

where,

P_TYPE : identifies the data packet

P_ID : a unique number used to identify duplicate packets

S_ADD : address of the sender of packet

D_ADD : address of the destination node

TTL : count of number of intermediate nodes traversed, limited to a ($2^4 = 16$)

LVN : list of addresses of previously visited nodes

TV : trust value of node between 0 to 10 as shows in Table I

It is assumed that the TV will be in the range 0-10 and the LOT is defined by accordingly. Based on LOT, security action is taken i.e. if a node is having low TV, then higher security action is required. Security actions according to LOT are assumed and given in Table I.

**Table I.** Security level assumption

| TV | LOT | Security Action (Required Encryption) |
|---|---|---|
| 9,10 | High | Low |
| 5,6,7,8 | Medium | Medium |
| 2,3,4 | Low | High |
| 0,1 | 0 | Packet drop (Malicious / Selfish node) |

Each node maintains information about its neighboring nodes by broadcasting a request packet. The format of request packet is shown in Fig. 2. Every recipient node adds the information of sender into a Neighbors Information Table (NIT). The neighboring nodes, which receive request packet in turn acknowledge the same by sending a reply packet. The format of reply packet is shown in Fig. 3.

| P_Type | S_add | D_add |
|---|---|---|

**Figure 2.** Format of request packet.

| P_Type | S_add | D_add | TV |
|---|---|---|---|

**Figure 3.** Format of reply packet.

In the repository, a node contains trustworthy and untrustworthy nodes based on the previous interactions. The TV is given by

Success Rate ($S_R$) of node i.e. (SR) = $T_s / T_{total}$

$T_s$ = Number of Packets successfully transmitted

$T_{total}$ = Total Number of packets transmitted

the overall trust of a node, if the node is participated 'n' times is calculated as follows equation:

$$TV = 1/n \sum_{j=1}^{n} SR \quad (1)$$

All the nodes in the MANET repeat this process until each node gives details about its neighboring nodes. This information is used by the nodes to forward data packets. Whenever there is a packet drop, NIT entries are updated. However, after a regular interval of time, every node within a cell retransmits a request packet in order to readjust the network information about its neighboring nodes. This process helps in maintaining a consistent network view.

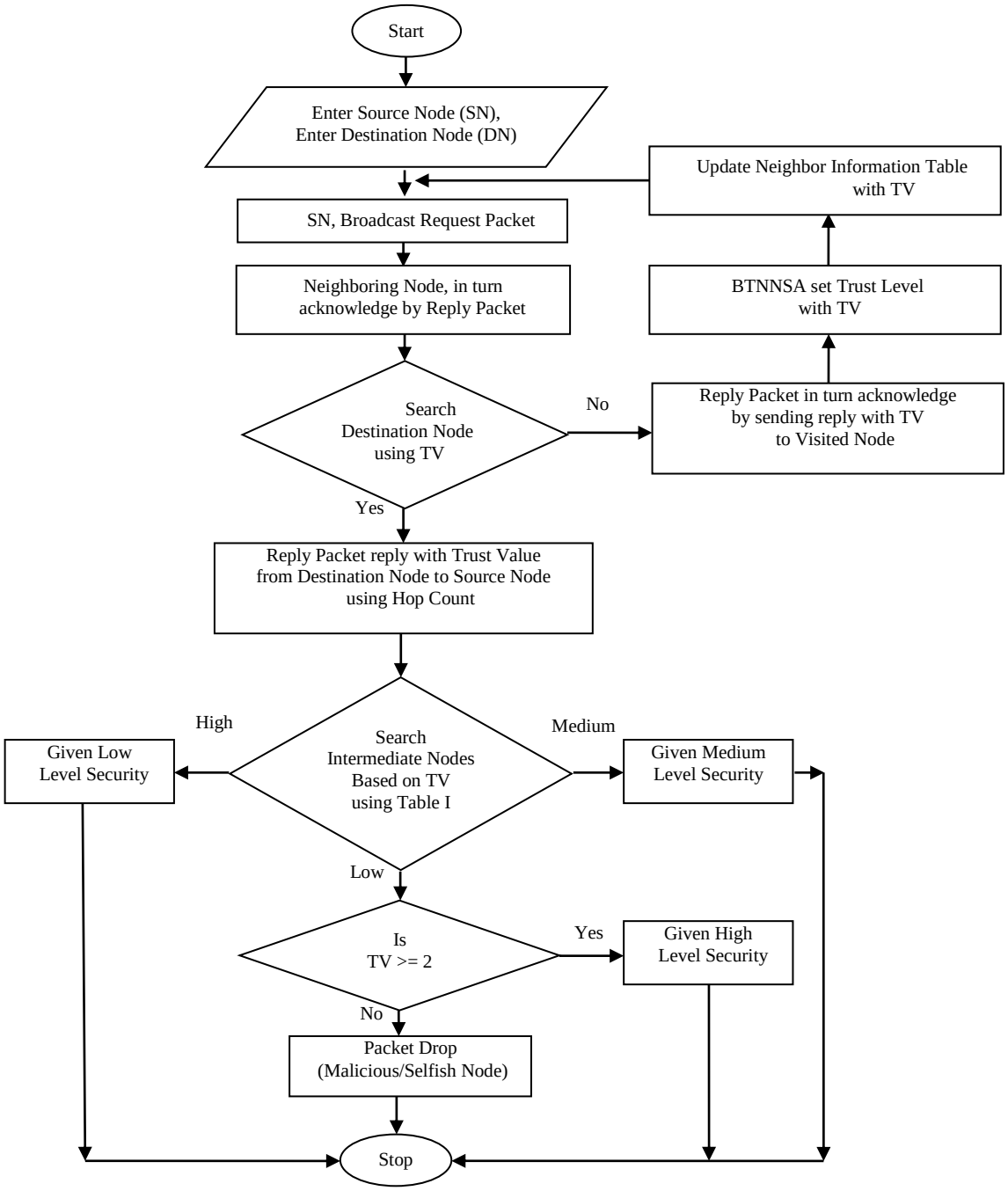



**Figure 4:** Flowchart of the proposed TBSRPM.

In order to provide the minimum number of nodes in between source to the destination, It finds the best neighbor node to which data packet can be transmitted. The priority is given to the node having higher TV. The RT function provides security level with respect to least TV of nodes as shown in security level assumption (Table I). Finally source node sends data packet to destination node. The flowchart of the proposed protocol is shown in Fig. 4.

## VALIDATION OF TBSRP

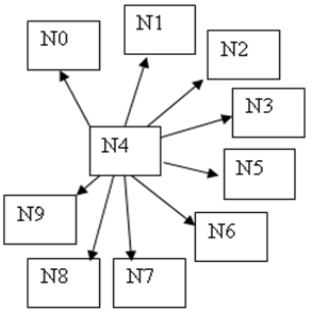
For validation of TBSRP protocol, four test cases have been discussed in this section. A network of 16 nodes is created. The SN and DN are set. The TV of each node is calculated with the help of Equation (1) as shown in Table II.

*Validation of algorithm*: To validate the above algorithms, multiple set of simulations have been performed and four test cases have been shown to validate the algorithm.

**Table II.** NIT entries of participating nodes

| Participated Node | Neighbor Nodes | TV |
|---|---|---|
| N0 | N1,N2,N3,N4,N5 | 1,3,2,10,5 |
| N1 | N0,N2,N3,N4,N5 | 2,3,2,10,5 |
| N2 | N0,N1,N3,N4,N5 | 2,1,2,10,5 |
| N3 | N0,N1,N2,N4,N5,N6,N7,N8 | 2,1,3,10,5,8,1,9 |
| N4 | N0,N1,N2,N3,N5,N6,N7,N8 | 2,1,3,2,5,8,1,9 |
| N5 | N0,N1,N2,N3,N4,N6,N7,N8 | 2,1,3,2,10,8,1,9 |
| N6 | N3,N4,N5,N7,N8,N9,N10,N11 | 2,10,5,1,9,8,10,5 |
| N7 | N3,N4,N5,N6,N8,N9,N10,N11 | 2,10,5,8,9,8,10,5 |
| N8 | N3,N4,N5,N6,N7,N9,N10,N11 | 2,10,5,8,1,8,10,5 |
| N9 | N6,N7,N8,N10,N11,N12,N13,N14 | 8,1,9,10,5,9,9,7 |
| N10 | N6,N7,N8,N9,N11,N12,N13,N14 | 8,1,9,8,5,9,9,7 |
| N11 | N6,N7,N8,N9,N10,N12,N13,N14 | 8,1,9,8,10,9,9,7 |
| N12 | N9,N10,N11,N13,N14,N15 | 8,10,5,9,7,7 |
| N13 | N9,N10,N11,N12,N14,N15 | 8,10,5,9,7,7 |
| N14 | N9,N10,N11,N12,N13,N15 | 8,10,5,9,9,7 |
| N15 | N12,N13,N14 | 9,9,7 |

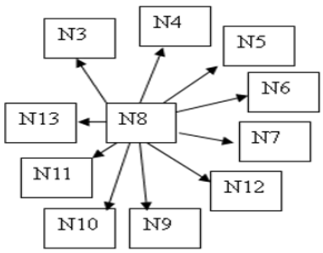
In case 1, the source node is set to N4 and destination node is set to N13. Node N4 broadcasts packet to all its neighbor nodes to find destination node N13 as shown in Figure 5(a). All nodes reply to source node N4 and update the NIT with TV.




Note: Source Node (N4) broadcast Packet to All near Neighbor Nodes. Now All near Neighbor Nodes calculate their Trust Value by using Trust Computation and update the Neighbor Information Table (NIT).

| Node | Trust Value |
|---|---|
| N0 | 2 |
| N1 | 1 |
| N2 | 3 |
| N3 | 2 |
| N5 | 5 |
| N6 | 8 |
| N7 | 1 |
| N8 | 9 |
| N9 | 8 |

(a)




Note: Node (N8) broadcast Packet to All near Neighbor Nodes. Now All near Neighbor Nodes calculate their Trust Value by using Trust Computation and update the Neighbor Information Table (NIT).

| Node | Trust Value |
|---|---|
| N3 | 2 |
| N4 | 10 |
| N5 | 5 |
| N6 | 8 |
| N7 | 1 |
| N9 | 9 |
| N10 | 10 |
| N11 | 5 |
| N12 | 9 |
| N13 | 9 |

(b)

**Figure 5(a-b):** Updation of NIT.

Node, which is having highest TV, now leads the network. At this moment N8 broadcasts to all its neighbor nodes as shown in Figure 5(b), and this procedure repeats in anticipation of the packet reach to its destination i.e. N13. Destination node N13 traverses back to source node N4 with reply packet along with the route information. Table III and Table IV shows the required security level and number of hop count based on TV.

Similarly in case 2, the source node is set to N11 and destination node is set to N4. The same set of operations has been repeated as shown in case 1. It is observed that in case 2 the required security level is medium as compared to case 1. Table III shows the required security level for all the four cases and Table IV, along with Figure 6, shows the required number of hop counts.

**Table III:** Security Level

| | Route Node | Time To Live | TV | Security Level |
|---|---|---|---|---|
| Case 1 | N4 | 1870 | 10 | Low |
| | N8 | 1875 | 9 | Low |
| | N13 | 1886 | 9 | Low |
| Case 2 | N11 | 382 | 5 | Medium |
| | N8 | 382 | 9 | Low |
| | N4 | 388 | 10 | Low |
| Case 3 | N3 | 910 | 2 | High |
| | N4 | 916 | 10 | Low |
| | N8 | 921 | 9 | Low |
| | N12 | 932 | 9 | Low |
| Case 4 | N1 | 421 | 1 | Packet Drop |
| | N4 | 426 | 10 | Low |
| | N9 | 437 | 8 | Medium |

**Table IV.** Number of HOP Count

| | Source Address | Intermediate Node | Hop Count | List of Visited Node | TV | Security Level |
|---|---|---|---|---|---|---|
| Case 1 | N4 | N8 | 0 | -- | 9 | Low |
| | | N13 | 1 | N8 | 9 | Low |
| Case 2 | N11 | N8 | 0 | -- | 5 | Medium |
| | | N4 | 1 | N8 | 5 | Medium |
| Case 3 | N3 | N4 | 0 | -- | 2 | High |
| | | N8 | 1 | N4 | 2 | High |
| | | N12 | 2 | N4, N8 | 2 | High |
| Case 4 | N1 | N4 | 0 | -- | 1 | Packet Drop |
| | | N9 | 1 | N4 | 1 | Packet Drop |

Overall it is observed that in test case 1, low security level is required. The required security level is based on TV. Similar test cases 2, 3 and 4 required medium, high and packet drop respectively. The proposed algorithm is the extension of existing reactive routing protocol (AODV) for creating secure route between sources to destination. The protocol behavior depends on TV and LOT as well as TV decides what level of security action is required. So based on TV, the data packet is encrypted. With the help of TV, malicious nodes can be easily eliminated and we can establish a best trusted route as well. Results show that the proposed algorithm enhances the security in the network.

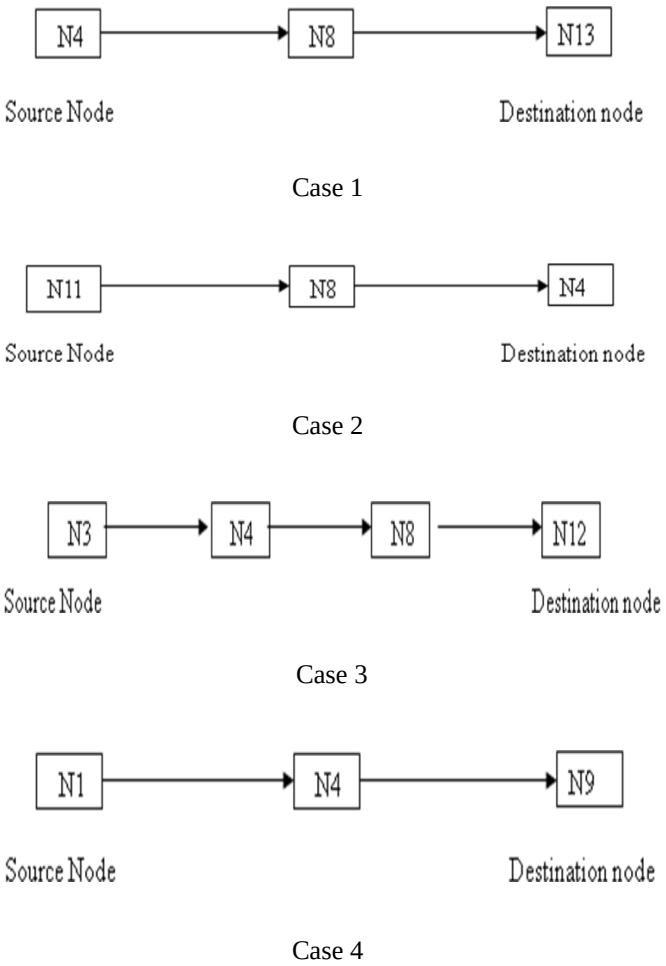



**Figure 6:** Number of hops between source to destination.

## CONCLUSION AND FUTURE SCOPE

In this paper, a trust-based secure routing protocol for MANETs has been proposed by the authors and to substantiate the protocol, four test cases have been discussed. With the help of this protocol, the required security level can be easily set up. This algorithm can also be easily integrated with various other reactive routing protocols like Dynamic Source Routing (DSR), Dynamic Source Distance Vector (DSDV) available for MANETs.

**ACKNOWLEDGMENT**

The authors wish to acknowledge Mr. Rohit Garg, Faculty Member, YMCA University of Science & Technology, Faridabad, Haryana, India, for valuable advice and moral support provided by him.

**REFERENCES**

[1] Mukesh Kumar Garg and Neeta Singh, "Routing and security issues for trust based framework in mobile ad hoc networks", IOSR Journal of Computer Engineering (IOSR-JCE*)*, e-ISSN: 2278-0661, p-ISSN: 2278- 8727, Volume 17, Issue 3, Ver. II (May-June 2015), PP. 01-05.

[2] Mukesh Kumar Garg and Ela Kumar, "Relative performance analysis of reactive (on-demand-driven) routing protocols", IJARCET International Journal of Advanced Research in Computer Engineering & Technology, Volume 3, Issue 12, December 2014, pp 4167-4172, ISSN: 2278- 323.

[3] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector (AODV) routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, February 1999, pp. 90-100.

[4] Manel Guerrero Zapata and N. Asokan, "Securing ad hoc routing protocols", In the Proceeding of 3rd ACM Workshop on Wireless Security (WiSe'02), Atlanta, Georgia, USA, ACM Press, September 28, 2002, pp. 1-10.

[5] Z. Yan, P. Zhang and T. Virtanen, "Trust evaluation based security solution in ad hoc networks", In the Proceedings of the Seventh Nordic Workshop on Secure IT Systems (NordSec 2003), 15-17 October 2003, Gjøvik, Norway.

[6] Asad Amir Pirzada and Chiris McDonald, "Establishing trust in pure ad-hoc network", Proceeding of 27th Australasian Computer Science Conference, ACM Int'l Conf. Proc. Series, Dunedin, New Zealand, 2004, Vol. 26, pp. 47-54.

[7] Xiaoqi Li, Michael R. Lyu and Jiangchuan Liu, "A trust model based routing protocol for secure ad hoc networks", In the Proceeding of IEEE Aerospace Conference (IEEEAC), 6-13 March 2004, Volume: 2, pp. 1286-1295.

[8] Rajiv K. Nekkanti and Chung-wei Lee, "Trust based adaptive on demand ad hoc routing protocol", ACMSE'04, April 2-3, 2004, Huntsville, Alabama, USA, ACM 2004, pp. 88-93.

[9] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya, "Trust based routing decisions in mobile ad hoc networks," in the Proceedings of 2nd Secure Knowledge Management Workshop (SKM), 2006, National Science Foundation and the Polytechnic University, Brooklyn, NY.

[10] D. Umuhoza, J. I. Agbinya and C. W. Omlin, "Estimation of trust metrics for MANET using QoS parameter and source routing algorithms", In the Proceedings of 2nd IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), 20-30 August, 2007, Sydney, Australia.

[11] Sultan Almotiri and Irfan Awan, "Trust routing in MANET for securing DSR routing protocol", ISBN: 978-1-902560-24-3 © 2010 PGNet.

[12] R. S. Mangrulkar and Mohammad Atique, "Trust based secured ad hoc on-demand distance vector routing protocol for mobile ad hoc network", 978-1-4244-9730-0/10/$26.00 ©2010 IEEE.

[13] Naveen Kumar Gupta and Kavita Pandey, "Trust based ad-hoc on demand routing protocol for MANET", Published in: Contemporary Computing (IC3), IEEE, 2013, Sixth International Conference on 8-10 August, 2013, pp. 225-231.