ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
March 2017,
Vol. 10, No. (1):
Pgs. 94-102

Security Enhancement of AODV Protocol using Fuzzy based Trust Computation in Mobile Ad Hoc Networks

ASHISH KUMAR JAIN[1]* and VRINDA TOKEKAR[2]

Institute of Engineering & Technology, Devi Ahilya University Khandwa Road, Indore (M.P.), India.
*Corresponding author E-mail: ajain@ietdavv.edu.in

http://dx.doi.org/10.13005/ojcst/10.01.13

(Received: February 18, 2017; Accepted: March 18, 2017)

ABSTRACT

Mobile ad hoc network (MANET) possess self-configuration, self-control and self-maintenance capabilities. Nodes of MANET are autonomous routers. Hence, they are vulnerable to security attacks. Collaborative attacks such as black hole and wormhole in MANET are difficult to be detected and prevented. Trust based routing decision is an effective approach for security enhancement in MANET. In this study, trust computingusing fuzzy based max-product composition scheme is applied to compute aggregated trust values to determine malicious nodes and thereby safe route in MANETs. The results show performance improvement ofproposed protocol over AODV protocol. Network metrics are analysed under different mobility conditions and different positions of black hole nodes.

Keywords: Blackhole attacks, Trust based computing, Fuzzy, MANETs, Trust formulation, Max product composition

INTRODUCTION

Wireless local area networks (WLAN) present unique and global way of networking with mobile nodes. WLAN were based on IEEE standards 802.11 a,b,g standards[1]. But, in most of the configurations of WLAN, only the last link is connected with access point thereby acting as wireless. Access point itself may be considered as bottleneck because of its limited range. There are many application areas such as battlefield communication, urban sensing and vehicular networking, where spontaneous communication is needed, WLAN may not be suitable, and hence infrastructure less networks are required.

Mobile ad hoc networks (MANETs) are infrastructure less network. In case of MANETs, the nodes have capabilities ofself- configuration, lack of central control and self-maintenance[2].

Collaboration among MANET nodes is a problematic issue for forwarding packets[2] as the nodes are autonomous routers. MANET nodes themselves forwards data packets among each other hence are vulnerable to many security attacks. Mobility of the nodes increases its vulnerability towards many collaborative attacks. Black hole and wormhole are two collaborative attacks on MANET.

Black hole node tries to show that there is shortest path towards destination node just sending Route Reply (RREP) immediately upon receiving Route Request (RREG)[3]. Black hole may become cooperative attack, when two or more nodes participate in the attack.

Worm hole is a cooperative attack, in which two malicious nodes form a fast tunnel between them. Thereby, both attackers collude together and fabricate a false route and cheat other nodes[4].

This problematic issue of collaboration among MANET nodes can be resolved using trust based computing.

In MANET, trustworthy routes can be established by eliminating malicious nodes using trust based computing approach[3]. Trust can be computed directly by a node for the other node or indirectly, when a node A recommends node B to the node C. Trust of a non-neighbouring node can only be computed indirectly. Hence, indirect trust plays a vital role in computing the overall trust of a node, which needs methods of trust propagation and trust aggregation. Hence, our approach is based on enhancing trust propagation and trust aggregation in order to evaluate trust, so that trustworthy routes can be established.

Trust computing is by default a fuzzy approach, as both of these are probabilistic approach. Hence, we are applying fuzzy approach in the proposed work.

This paper proposes fuzzy based trust computation to mitigate black hole attack in MANETs. Thus enhancing security of AODV routing protocol in MANETsmodel required to secure routing protocol of MANETs. We discuss related work in section II.We propose fuzzy based trust computation model to detect black hole attacks in section III. In section III, we also present several trust relation properties useful for trust based computation in MANETs. Section IV presents results and performance evaluation of simulated fuzzy based trust computation system. Finally conclusion is given in section V.

Related Work

HoanLan *et.al.* in[5] have demonstrated that the impact of black hole attack is catastrophic and it is malicious node position dependent. If the malicious node is near the source node then it has most damage to the network performance. The network performance is also highly dependent on the speed of mobile node.

Karim Konate *et.al.* in[6] have simulated black hole and grey hole attacks in terms of parameters like, number of packets sent and received, number of packets lost and consumption of energy. Authors have demonstrated that the rate of packet lost increase almost to 75% when the number of packets sent increases. Authors have discussed that the goal of black hole attack is to forward the data packets and not the routing packets.

Jin Hee Cho *et.a.l* in[7] have shown the survey on Trust Management for MANETs. Authors have demonstrated multidisciplinary concept of trust. Authors have discussed trust in sociology, Economics, Autonomic computing, organizational management, psychology and philosophy. Authors have defined trust management as a special case of risk management.

Mousumi Sardar *et.al.* in[8] have shown trust for secure routing in MANETs. Authors have calculated trust of node as an average of neighbouring nodes opinion. Authors have shown that the attacker node can send false alarm message for claiming a good node to be bad node to isolate the normal node. In this way mischievous node can be detected.

Baptiste Alcalde et.al. in[9] have shown that the trust and risk management are concurrent research areas. Authors have developed a decision model for trust and security risks. Authors have developed a new trust model based on risk model. But this model does not show the metrics of risk management. They have also not shown the trustor's risk resulting from consequences from several decisions in trust management.

Asad Amir Pirzada *et.al.* in[10] have presented model for trust based communication in pure ad hoc networks. Authors have represented trust as continuous value as the MANETs are topologically indynamic state. Authors have computed trust based on events that can be recorded in passive mode. But their model is suited only for pure ad hoc networks.

Weighted Binary Relational Fuzzy Trust Model

Trust should be a necessary element of distributed systems which depends on relationship between different entities of the distributed systems[5]. Trust is a reliance of one entity to the other. It depends on the first entity that how much it believes in second. An entity may rely fully on the other entity. But in practical scenario this is not possible. Therefore, trusts can be modelled as a probabilistic value, which can be denoted as a fractional value between 0 and 1. Hence, Trust computation approach is by default a fuzzy approach.

Trust can be modelled mathematically as a binary relation on A×A, where A is a set of nodes in MANET. This binary relation is weighted as the weights of this relation are fractional trust values of one node to the other node. These weights represent the extent to which a node believes in other node.

Properties of Weighted Binary Relational Fuzzy Trust Model

The different properties a relational trust model satisfies are described as follows:-

1. **Dynamic**
   Nodes of MANET are mobile in nature; therefore computed trust should be based on spatial local information. Such kind of information can change rapidly[11]. Hence trust should be dynamic. Dynamic variables should be treated as continuous variable. Hence trust value is kept as continuous value ranges in [0,1].
2. **Reflexive**
   Trust has to be a reflexive relation as a node has to trust itself. Consider Cartesian product A×A. T is a trust relation on this product. That means $T \subseteq A \times A$. Let us consider a node N. So, T(N,N)=1, that means a node fully trust itself. So, the relation has to be reflexive.
3. **Asymmetric**
   This relation, consider two nodes N and M. Both of them may not trust each other with equal extent. So, the relation has to be asymmetric essentially.
4. **Weighted Transitive**
   A relation is said to be transitive when first party trusts second party and second trusts third party. Let us consider nodes A,B and C in trust relation. If trust value T(A,B) denotes trust value of node A for node B and T(B,C) denotes trust value of node B on node C. Then trust value of node A on node C T(A,C) can be calculated using the values T(A,B) and T(B,C).

   In MANETs, trust value of strange node is computed based on previous trust values of neighbouring nodes. As trust based computation need inferences of neighbouring nodes to compute trust of another node. Hence trust relation is considered as weighted transitive relation.
5. **Personalization relation**
   It defines perception about trust of a node by another node. It is defined in terms of trust value which ranges between 0 to 1. A fuzzy discrimination table is defined to represent the behaviour of node in terms of its trust value (Tab 1).
6. **Subjective**
   In dynamic environment of MANETs, trustor node may observe different opinion of a node at different time instances. Hence trust is said to be subjective to a condition[11].
7. **Context Dependent**
   'A' may trust 'B' as student but may not trust as employee. In MANETs also, there are different types of trust relations are required for different tasks. For example the trust value of a node for packet forwarding capability may notrepresentits reporting capability[11].
8. **Composability**
   Trust value received from different routes can be composed together to obtain a single opinion value. This property is to be used to calculate aggregate value of trust.

Trust Based Computing

Nodes of MANET have to trust other nodes of same network. But, all the nodes are not equally trustworthy. Some nodes are selfish, some might be malicious and others might be completely trustworthy. Hence, trusted computation should be used to detect the behaviour of node.

Trust computation in static networks is straightforward as trust values vary only with the behaviour of the node. After some observations behaviours and trust values are predictable[2]. Trust computation in mobile networks is considerably difficult as compared to static networks, as compromised node may move after attack and it will be very difficult to detect such malicious node[2]. Network topology significantly changes within time in a volatile manner. Hence, observations for neighbouring node are difficult. Behaviour of a node is predictable only after enough number of observations. Furthermore, it is difficult to associate a mobile node with its location and gaining observations. MANETs are peer-to peer networks, there is absence of centralized control station and observing the behaviour of node becomes very complicated.

1. Trust Formulation

Trust is to be formulated by one entity for the other. This formulation might be guessing an opinion of other entity. Mathematically, trust is probability of trustworthiness of one entity about the other. In case of MANET, it is required to compute the trust value by one node for the other node. MANET is an open network; any node can join and leaves the network at any time. When a new node joins the network, the trust with some default value is initialized. For the new node, the default value for the trust will depend upon the application where MANET is used. The trust will keep on changing over the time based on the feedback obtained from other nodes. Trust computation of node about neighbouring node will depend upon certain parameters. These parameters may include, packet delivery ratio of a node, percentage of energy exhaustion of node, percentage of Buffer utilized by the node and number of connection request given by node.

2. Trust Propagation

A node computes trust for a target node and transmits that trust value to its neighbouring nodes, so that neighbouring nodes save time and resources of recomputing the trust values for the same node[2]. Consider, fig 2, in the network there are five nodes A, B, C, D and E. A computes trust value denoted as T (A, B) for the target node B. B computes T (B, C) for the node C. C computes T(C, D) for node D and D computes T (D, E) for the node E. Node A needs the trust value of E, for that D propagates T (D.E) to C and then C propagates T (D, E) to B and then to the trust requesting node A.

3. Trust Aggregation

Nodes of MANET are propagating trust values to their neighbours. Node might get multiple values of trust for any target node. So, aggregation of trust is often needed to be computed. Aggregate value of trust is to be calculated via trust path. Malicious node in between the trust path can change the values of propagated trust. So, multiple paths for the aggregated trust are to be considered.

Trust Aggregation using Max-Prod Composition of fuzzy Relations

Trust composition is used to aggregate the trust value by the operation called “Composition”. This method uses product of two matrices with their maximum fuzzy trust values called Trusted Maximum Product composition of fuzzy relations (TMPCF). Let us consider three N×N matrices A, B and C which stores fuzzy trust values.

Let α (x, y), (x, y ε A × B) and β(y, z) , (y, z ε B× C) be the two relations. The proposed

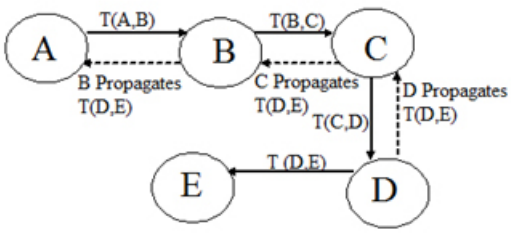

Fig. 2 : Trust propagation

approach is used to calculate the aggregate trust value. The trust values, which were propagated by a node to their neighbouring node forms a binary relation and recorded as N×N matrix. These propagated trust values are aggregated to form aggregated trust value.

The TMPCF approach used to calculate aggregate trust is the fuzzy set

$$Aggtrust(x,z) = Max_y \{\prod \{\mu\alpha(x,y), \mu_\beta(y,z)\}\}$$

Where $x \varepsilon A, y \varepsilon B$ and $z \varepsilon C$ ...(1)

Here μ_α and μ_β are membership function of a fuzzy relation on fuzzy sets.

In our earlier research[12], we have proposed direct trust computation method as depicted in eq (2)

$$T(A,B) = \sum_{i=1}^{n} (w_i x_i(A,B)) \quad ...(2)$$

Such that $\sum_{i=1}^{n} w_i = 1$

Where Node 'A' calculates trust of node 'B' based on the parameters like packet forwarding ratio of node, energy exhaustion, buffer utilization and number of connection request. Final trust value is calculated based on aggregated trust and direct trust, which is depicted in eq (3).

$$T(i,j)=Aggtrust(i,j)*trust_{factor} + directtrust(i,j)*(1-trust_{factor}) \quad ...(3)$$

Where 0<trust_factor<1

METHODOLOGY

The proposed protocol Trusted Fuzzy Ad hoc on demand distance vector routing protocol (TFAODV) uses TMPCF approach to calculate aggregated trust. This aggregated trust with direct trust between the nodes are used to calculate trust value as depicted in (3). The trust value derived is used in the proposed protocol TFAODV. TFAODV uses trust computation approach, which is based on trust formulation, trust propagation and trust aggregation. Nodes get direct trust values from their neighboring nodes and aggregated trust values from non-neighboring nodes. Afterwards, nodes compute aggregated trust value using trust aggregation. This aggregated trust value is used to detect malicious node. The classification of node is completed using fuzzy discrimination table Tab 1. If the trust value drops to fuzzy level of low and very low, then that node will be considered as malicious and discarded from routing. If the aggregated trust value false in the range of medium, high and very high then the node will be used in routing activities.

Performance Analysis

Performance Metrics

Three performance metrics are assumed for analysis of TFAODV protocol Packet delivery ratio (PDR), Average End-to-end Delay (ETD) and

Table1: Fuzzy discrimination table for node behaviour

Trust value	Fuzzy Levels	Node behaviour
0-0.2	Very low	Malicious node
0.2-0.4	Low	Selfish Node
0.4-0.6	Medium	Normal Node
0.6-0.8	High	Co-operative node
0.8-1	Very High	Trustworthy and co-operative node

Table 2: Input Parameters For Black Hole Attack Under Aodv &Tfaodv

Simulation Time	900 Seconds
Area	1km x 1km
Total Number of Nodes	50
Mobility Model	Random Waypoint
Transmit Range	250m
Packets transmission rate	8 packets/ sec
Packet size	512 bytes
Max no of packet per connection	10000
Traffic Type	CBR
Speed of node	0m/s (stationary) 1 m/s (low) 5m/s (moderate) 10 m/s (high)
No of malicious node	1 to 15 (2% to 30%)

Throughput. These network metrics are evaluated for both the protocols AODV and TFAODV under varying network conditions.

The simulation was carried out using NS2 as simulator with input parameters as given in table 2.

Various scenario files and network animations files are created by varying the number of nodes, malicious node's position, speed and duration of simulation. Finally, the output in terms of traces is generated for each scenario for both protocols. Awk file is used to evaluate network performance metrics.

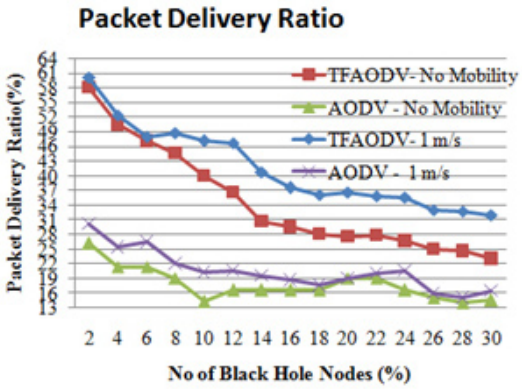

Fig. 3: Packet Delivery Ratio for stationary and low mobility

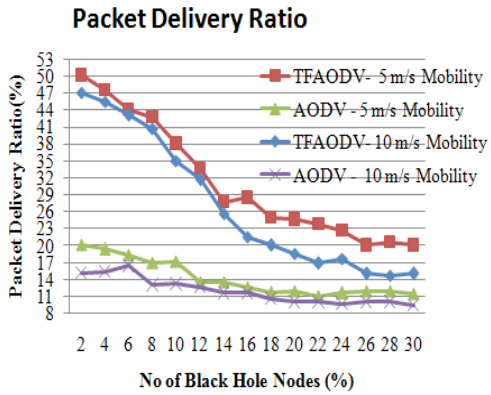

Fig. 4: Packet Delivery Ratio under high mobility

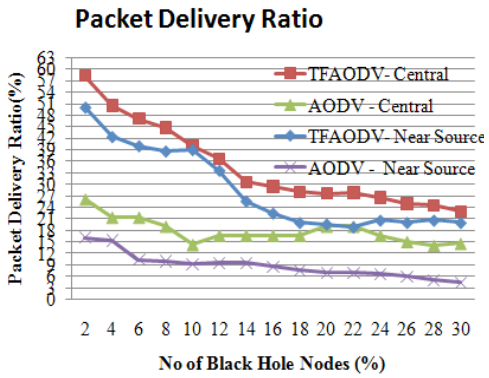

Fig. 5: Packet Delivery Ratio with different positions of malicious nodes

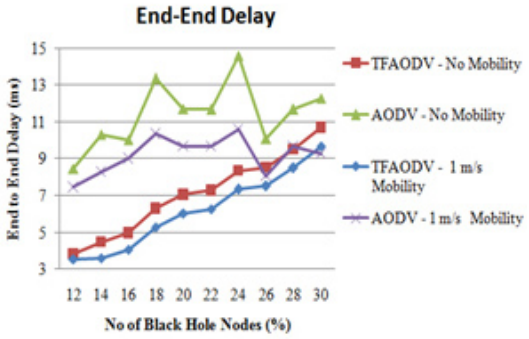

Fig. 6: End to End delay under low and moderate mobility

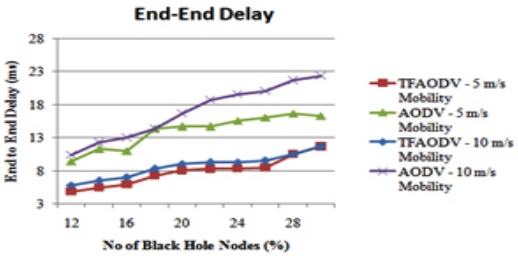

Fig. 7: End to End delay under high mobility

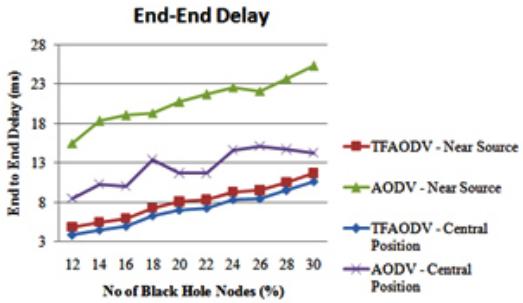

Fig. 8: End to End Delay under different positions of malicious nodes

Network performance values are evaluated on each scenario under different network conditions as a function of number of malicious nodes. The nodes of network have varying mobility, thereby one of the scenarios is considered to be the speed of nodes. Some of nodes might be stationary and others are moving with varying speed. Hence, the first scenario consists of stationary nodes as a comparison with that of low mobility of 1 m/s. These scenarios are depicted in the fig 3, fig 6 and fig 9 for PDR, ETD and throughput respectively. Nodes might be having high mobility with speed of 5 m/s and 10 m/s, these scenarios are represented in fig 4,7 and 10 for PDR, ETD and throughput respectively. Malicious nodes positions are considered, nodes might be positioned at near the source and at centre of the terrain. These scenarios are depicted in fig 5,8 and 11 for PDR, ETD and throughput respectively.

RESULTS

Fig 3, shows PDR for low mobility and stationary nodes. Clearly TMPCF have outperformed AODV in terms of PDR under this case. Furthermore, TMPCF's PDR under low mobility of 1 m/s is also outperforming stationary node's PDR may be because malicious node may not be in completely contact with victim nodes always, which is possible in stationary node case. Hence, network performance due to malicious nodes may be improved in low mobility case as compared to stationary case. Same behavior is also observed in case of throughput and ETD parameters as seen in fig 6 and 9.

Fig 4, fig 7 and fig 10 shows PDR, ETD and throughput under high mobility of 5m/s and 10 m/s of nodes. Clearly TMPCF outperformed AODV, but because of high mobility there may be some link breaks occur, so at mobility of 10 m/s performance of both protocols deteriorates.

Fig 5, fig 8 and fig 11 shows PDR, ETD and throughput under different positions of malicious nodes, positions of normal nodes are random. The node's positions are taken as central to the complete terrain area and near the source

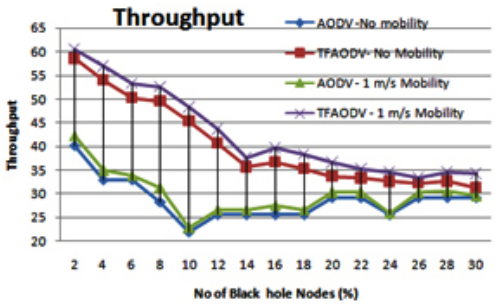

Fig. 9: Throughput under low and moderate mobility

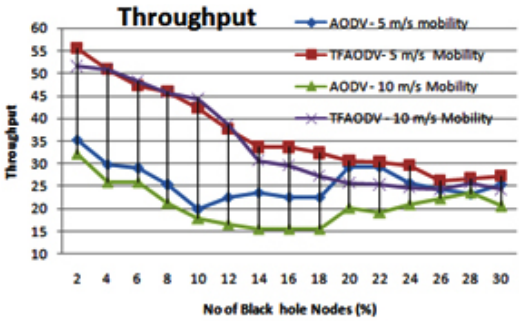

Fig. 10: Throughput under high mobility

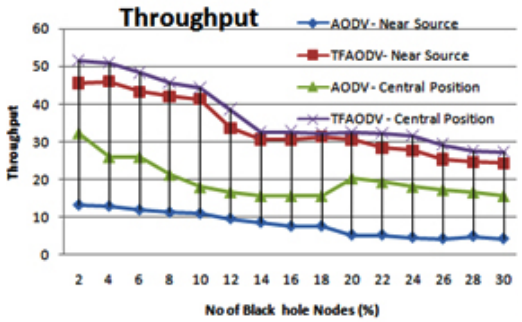

Fig. 11: Throughput under different positions of malicious nodes

node. Performance under these scenarios shows, that when malicious nodes are near to the source node, performance deteriorates because malicious node is in contact with the source node and drop packet immediately it receives. But, in this case too TMPCF's performance saw some enhancements over AODV under any position of nodes.

CONCLUSION

MANET is infrastructure less network and operates in untrusted environment. In the proposed work TFAODV, we have given solution of black hole attack in an untrusted environment of MANET using TMPCF approach. Our work uses fuzzy based trust computation approach. Network performance of MANET varies on conditions such as node mobility and positions of malicious node in the terrain. The proposed work considered different mobility conditions such as stationary network, low, moderate and high mobility nodes of the network. The position of malicious node considered are also different, central position and near source node in the terrain.

The performance of MANET under low mobility is better as compared to stationary nodes, as stationary nodes are more vulnerable. MANET performance in case of malicious node central position in terrain is better as compared to near the source node, as malicious node near the source may directly attack and thus reduce the performance. Hence, our result shows that the proposed approach, TFAODV have outperformed AODV under all conditions in terms of network performance.

REFERENCES

1. Azzedine Boukerche , Begumhan Turgut, Nevin Aydin, Mohammad Z. Ahmad, Ladislau Bölöni, Damla Turgut , "Routing protocols in ad hoc networks: *A survey", Computer Networks,* **55**, pp 3032-80, 2011
2. Farrukh Aslam Khan a,c,", Muhammad Imran b,c, Haider Abbasa,d, Muhammad Hanif Durad, "A detection and prevention system against collaborative attacks inMobile Ad hoc Networks", *Future Generation Computer Sysmtems*, **68**, 2017, pp 416-427
2. Kannan Govindan, Prasanna Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey",
3. J.Manoranjini, A.Chandrasekar, D.Rajinigirinath, "Hybrid Detector for Detection of Black Holes in Manets", IERI Procedia, pp 376 – 3822013 International Conference on Electronic Engineering and Computer Science,
3. Krishnaprasad Thirunarayan, Pramod Anantharam", Cory Henson, Amit Sheth, "Comparative trust management with applications:Bayesian approaches emphasis", *Future Generation Computer Systems*, **31**, pp 182-199, 2014
4. Hao-Ting Pai, Fan Wu, "Prevention of wormhole attacks in mobile commerce basedon non-infrastructure wireless networks", *Electronic Commerce Research and Applications*, **10** , 384–397, (2011)
5. Hoang Lan Nguyen, Uyen Trang Nguyen, "A study of different types of attacks in mobile ad hoc networks " 25th IEEE Canadian conference on Electrical & Computer Engineering, 2012
6. Karim Konate, Gaye Abdourahime, "Ättacks analysis in mobile ad hoc networks: Modelling and Simulation", second international conference on Intelligent systems, modelling and simulation, 2011
7. Jin Hee Cho, Anantram Swami, Ing Ray Chen, "A survey on Trust Management for Mobile Ad hoc Networks" IEEE *Communications Surveys and Tutorials*, **13(4)**, pp 562-581, Fourth Quarter 2011.
8. Mousami Sardar, Koushik Majumdar, "A survey on trust based secure routing in MANET", ICCSEA, SPPR,CSIA, 2013
9. Baptiste Alcalde, Eric Dubois, Sjouke Mauw,

Nicolas Mayer, Sasa Radomirovic, "Towards a decision model on trust and security risk management", in proceedings of 7th Australasian Information security conference (AISC 2009), Wellington New Zealand

10. Asad Amir Pirzada and Chris McDonald, "Establishing Trust in Pure Ad hoc Networks", 27thAustraliasian computer sc. Conference, 2004

11. Simin Hall, William McQuay, "Fundamental Features of a Unified Trust Model for distributed systems",

12. Ashish Kumar Jain, VrindaTokekar, "Security Enhancement in MANETs using Fuzzy based Trust Computation against Black hole Attacks", *International congress on Information Communication Technology*, 12-14, 2016.