Trust based Ad-hoc On demand Distance Vector Routing Protocol

Raghvendra Sahu[1] and Jimmy McGibney[2]

[1] MSc Communication Software, WIT
[2] WIT

Abstract. Ad-hoc networks are boundaryless and can be accessed by untrusted agents. These agents may participate in routing and can make the network hostile. In this paper I have proposed a protocol that uses trust as a routing metric in ad-hoc networks. The protocol implements all the features of AODV. It uses trust to calculate the most reliable route. I have also proposed an algorithm to calculate behaviour of a node. There are three parameters which define the behaviour of a node. Two of them define benign or malicious behaviour. The third parameter defines the impact of behaviour on the network. This parameter is used to control the security level of network. The proposed protocol is shown to generate 20% less route discovery control packets than AODV, under certain experimental conditions[3]. With the help of simulations I have demonstrated that the proposed protocol generates less control traffic, isolates malicious nodes and finds reliable routes. These features provide an advancement over existing AODV as well improving route reliability in hostile ad-hoc networks.

1 Introduction

In recent years mobile ad-hoc networks(MANETs) and wireless networking devices have gained popularity. They can often be used in "scenarios where no infrastructure exists or in which the existing infrastructure cannot meet the requirement of application based on security and cost"[19]. Extensive work has been done in recent years to integrate these elements with traditional network such as wired Internet. While these research efforts initially assumed a friendly and cooperative environment[13] and focused on problems such as wireless channel access and multi hop routing, providing a protected communication between the nodes have become the primary concern in today's hostile environment. Although security has been an active topic in wire-line networks, but the unique characteristics of MANET has presented a set of non trivial challenges to security design. These challenges include *open network architecture, highly dynamic network topology, shared wireless medium, lack of infrastructure.* Consequently security solution of existing networks do not apply to MANET. Each node in MANET is an end system as well as a router to forward data. The behaviour

[3] See table Simulation Variable

of node is important for successful routing. A node can be benign or malicious. Benign nodes actively participate in routing and honestly forward the data to other nodes while malicious nodes drop packets or flood network with routing traffic.

AODV is one of the routing protocols that defines set of rules to forward data in MANET. This protocol assumes all nodes are benign and can be trusted for honest routing[19]. However, wireless nodes have limited resources and sometimes they violate the protocol to conserve their resources, resulting in disrupted routing. These nodes are termed as malicious nodes.

Malicious nodes can be selfish or they may be compromised. Selfish nodes are reluctant to participate in routing and they can drop forwarded packet. Experiments have shown this behaviour degrades the performance of AODV[3], so it is important for a benign node to determine the behaviour of other nodes. The rest of this section describes the AODV protocol and trust.

1.1 AODV

AODV is an on-demand routing protocol. AODV scales to more than 10,000 nodes easily [13].It builds routes between nodes only as desired by source nodes. It is loop-free and self-starting. This protocol uses RREQ to find a route.

Route Building – RREQ A node initiates the process of route discovery only when it needs a route to destination. It disseminate a RREQ packet. This RREQ is received by one of its neighbour nodes. The neighbour node checks received RREQ to determine whether it has already received a RREQ from the same source. If such RREQ has been received then it discards the received RREQ. If this is a new RREQ then it forwards to other nodes setting up a pointer in routing table to previous hop. While forwarding RREQ intermediate nodes increase the hop count header in RREQ packet by one.

RREP As the RREP propagates back to the source, nodes set up forward pointers to the destination [13]. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop-count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained.

Route Maintenance and RERR A route is considered to be active as long as there is data transmission on that route. As soon as the route becomes idle, it gets deleted from routing table of intermediate node [13]. If any link between nodes of route is broken then node propagates a route error RERR message to *source node* to inform that route to destination is unavailable. If source node desires to send data to mentioned destination then it can re initiate route discovery.

1.2 Trust

Trust is a social concept. This is level of faith of one entity on another. It is built by observing the behaviour of another entity. Depending upon scenario trust change can be low or very high.

> Definition of Trust inspired by McKnight and Chervany (1996) [11]
> **Decision Trust**: Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

AODV assumes that all the nodes in network are benign. However, malicious nodes are also present in the network. It is important for the benign nodes to have the knowledge of malicious node in the network and they should not trust them for routing. I have used *decision trust* to isolate malicious nodes from routing. The concept of trust used in this paper is same as defined by Josang in [8].

The rest of the paper is organised as follows. In Section 2, I have discussed about using trust in AODV to find a route. I have given an overview of related work in Section 3. Section 4 elaborates the proposed protocol – Trust Based Adhoc On demand Distance Vector Routing Protocol (TBAODV). The simulation design and network configuration is done in Section 5. The results obtained in Section 6 demonstrates the effectiveness of TBAODV. TBAODV can reduce the routing traffic and improve route reliability. Conclusion and future work is in last section.

2 Problem Statement

Mobile Ad-hoc Network (MANET) does not have dedicated infrastructure to support routing. It uses intermediate nodes in the network for all communication among nodes. The behaviour of intermediate nodes is deciding factor in successful communication between two nodes. If the behaviour of intermediate nodes is benign then the route found will be secure for communication. Alternatively the behaviour of node can be malicious. Determining these behaviour is one of the problems which will be addressed in this paper. Apart from that this behaviour will be quantified.

The benign and malicious behaviour is defined by trust value, when a node shows malicious behaviour its trust value is decreased alternatively it can be increased if it shows a benign behaviour. The concept of trust is used to eliminate malicious nodes from routing. If malicious nodes are eliminated then performance of MANET will improve. The metric for performance evaluation of a MANET is given in Section 6. The performance of a MANET is improved by reducing the volume of routing traffic accompanied by reduction in packet loss[16]. Packet loss in this context is number of packets that never reaches to its destination. Further in this section I have elaborated behaviour mapping followed by trust calculation and route selection.

2.1 Behaviour Mapping

A node in MANET does not know about behaviour of other nodes within its power radius. It becomes necessary for a node to know about them. As behaviour is a qualitative factor. It is difficult to define a single solution to quantify behaviour of a node. However I have defined behaviour constants that can quantify the behaviour of nodes in the network. The behaviour in this context stands for the its benign quality and malicious quality. This benign quality has a value of more than one. High value of benign quality corresponds to highly trustable node. The benign quality is parameter defined by χ. This parameter is used to update the trust. It is used to imitate (measure or map) quality into quantity. In section 4 I have proposed behaviour constants. The behaviour of a node can be monitored by validating control messages during a transaction.

For malicious nodes α is used as behaviour constant. The possible values of alpha is given in Table 1. The selected values may not be suitable for all the network. I have used them in simulation to detect malicious nodes.

The behaviour will be an input for trust calculation. This trust will be used as a metric in route calculation. The next problem I have address is how to use the trust value as a routing metric. The behaviour of participating node can change with respect to time. To address this issue I have used Exponential function to update trust[9]. The trust is updated after transaction of packets. Receiver node detects the behaviour of sender node by validating the fields of control packet forwarded to it [13].

2.2 Updating and Initialising Trust

An Ad-hoc network can split into two or more different network and vice versa. This leads to a new challenge introduction of new nodes in the network. New node can have a trust value equal to threshold trust (τ). If a node sends data using new node and new node shows some malicious behaviour then its trust value will be decreased. I will use exponential algorithm to decrement the trust.The algorithm will use malicious and benign behaviour constants to map corresponding activity. The constants used are described in Table 1. Trust calculation for a malicious

Table 1. Constants and its Description

Constant	Description	Range
α	Malicious behaviour constant	$1 \leq \alpha$,
β	Security Level	$\beta > 0$
τ	Trust Threshold Value	$0 \leq \tau \leq 1$
χ	Benign behaviour constant	$\chi \geq 1$
n	Current State	$n \in$ { Non Negative Integers }

node is defined by Equation 1

$$Trust_{n+1}(\alpha) = \frac{Trust_n(\alpha)}{\alpha^{\beta}} \tag{1}$$

Equation 2 shows the initial trust value of new node.

$$Trust_0(\alpha) = \tau \tag{2}$$

Equation 3 calculates the trust value for a node , after it has shown first malicious activity,with behaviour constant of α.

$$Trust_1(\alpha) = \frac{\tau}{\alpha^{\beta}} \tag{3}$$

β represents the security level in the network. α is constant for a malicious activity. This function will be triggered after every malicious activity.For my simulations I have defined six security level. It has integral value from zero to six. Level zero security will behave like AODV while level five security is maximum.

When the new node shows benign behaviour a different algorithm will be used. The new trust value is calculated as per Equation 4.

$$Trust_{n+1}(\chi) = 1 - \frac{1 - Trust_n(\chi)}{\chi^{\frac{1}{\beta}}} \tag{4}$$

From Equation 2, initial trust value of new node is given by Equation 5

$$Trust_0(\chi) = \tau \tag{5}$$

Equation 6 shows the trust value of node, after it has shown first benign behaviour.

$$Trust_0(\chi) = 1 - \frac{1 - \tau}{\chi^{\frac{1}{\beta}}} \tag{6}$$

χ is behaviour constant. The benign behaviour corresponds to packet forwarding[19]. The value of χ for this behaviour is 1.5, Table 1. The selected value of χ may not be appropriate for all the networks. This value gives a converging solution for trust update in simulation. I will consider benign behaviour if the field of disseminated RREQ packet and corresponding RREP are valid.

There are many malicious behaviour. However, I will consider following attacks: *RREQ Flooding, Unreliable Node and Selfish Node.* In first two type of security attack the packet never reaches its destination. Selfish nodes can be of two types:First type forwards the routing packet but does not forward the data packet. Second type doesnot forward routing packet which are not of its direct interest. I have considered second type of selfish node in my simulation and results.

2.3 Route Selection

A route is path between source node and destination node via intermediate nodes. The number of intermediate node is defined as hop count. AODV selects route that has minimum hop count[13]. Low value of hop count increases the responsiveness of route. For a destination multiple routes can be found. Only that route is selected which is more secure. The security of this route is determined by the trust of nodes in the route. The overall trust of the route is important to route selection. Sensible calculation of overall trust is critical to application of trust as this can increase the hop count.

3 State of the art

Establishing security in AODV based on trust system is an important consideration. Some of the existing protocols related to my work have been discussed in this section. These protocols secure the control packets while I have considered isolating misbehaving nodes.

3.1 Security in mobile ad-hoc networks

The references [3, 12, 19] elaborate most of the security issues associated with mobile ad-hoc networks. The authors of these papers clearly state that *AODV* has *no security mechanism.*They have discussed about forging of control packets. Any malicious node can impersonate other node by forging RREQ with its originator address. It can also forge the RREP packets with its address as destination address. It can also not forward the RREQ or RREP packets. Authors in these paper have provided solution to secure the control packets. Securing control packets can not isolate malicious nodes from network.

Secure Ad-hoc On Demand Distance Vector Routing Secure Ad-hoc On Demand Distance Vector (SAODV) protocol secures the control packets[4] of AODV. It uses digital signatures to authenticate the non-mutable fields of the control messages and the hash chains to secure the hop count information. This approach assumes the nodes have access to key management system so that the nodes can obtain the public keys of the other nodes within the network.

In SAODV the routing information is authenticated that ensures that control message is from a reliable source.

Security Aware Routing Protocol The Security Aware Routing (SAR) Protocol described in [18] defines trust levels to establish security in AODV. SAR works for reactive routing protocols, this algorithm is equally applicable to DSR as well. In SAR route request and route reply packets are assigned a security level by the source node. Only nodes with at least indicated level of security can

[4] Collective term for Route Request and Route Reply Packets

process and forward the control messages. Hence, SAR discovers routes in which all nodes along the path meet the desired level of security.

I have followed a similar approach. But each node is not assigned a trust value or level, instead nodes calculate trust value for their neighbour nodes based on observation. The process of initialising and updating trust is not described in SAR. However, I have proposed some algorithms to achieve this.

3.2 Fuzzy based trusted AODV

In [15] author proposes "Fuzzy based trust model integrated with AODV reactive routing protocol". This model consists of four component

1. Trust Verification
2. AODV protocol
3. Fuzzy input parameter extraction
4. Fuzzy based trust computation

Trust verification component verifies the trust worthiness of neighbour from which it receives a control message. Third component observes the behaviour of neighbour nodes. This observation is based on directly experienced events. In fourth component they have used Mamdani based fuzzy model to compute trust. I have followed a similar approach. I am using exponential averaging function to calculate trust.

4 Solution

In a network there can be two type of node benign and malicious. The network is said to be attacked only when malicious node is present. The proposed protocol TBAODV isolates malicious node from routing, in an attacked network. TBAODV detects malicious node by validating control packets. It isolates them from routing for certain time. It uses trust value to calculate the best possible route. The routes with low hop count[13] and maximum overall trust are defined as best routes.

TBAODV maintains a neighbour trust table. All the directly experienced events with neighbours updates the values in table. The trust value lies between zero and one [9].

$$Trust \in [0, 1).$$

Minimum value of a trust can occur as result of more malicious behaviour than benign behaviour. The node showing more malicious behaviour has lower value. The trust value of zero represents complete distrust. Trust value of 1 represents complete trust. The upper limit for trust value never reaches 1.

4.1 Behaviour mapping

In MANETs a node can show multiple behaviour. The malicious behaviours which are discussed are tabulated in Table 2. These values are selected based on exponential function as in Equation 1. The plot for the each malicious activity is shown in Figure 6. The choice of α decides the convergence of function. If the behaviour is more malicious the rate of convergence is faster.

4.2 Trust Update and Malicious Node Isolation

The function used to update trust is shown in Equation 4 and 1. The function used to update trust in Equation 4 has a negative feedback. The new trust is obtained from previous trust. This function will never reach a value of 1. Similar function has been used to update trust in [9]. The author in [9] has used Exponential averaging function to update the trust. If security level is

Table 2. Behaviour Mapping

Behaviour	**Range of α**	**Value of α**
RREQ Flooding	$1.01 \leq \alpha \leq 1.1$	1.05
Unreliable Nodes	$1.11 \leq \alpha \leq 1.2$	1.15
Selfish Node	$1.21 \leq \alpha \leq 1.3$	1.25
Unexpected Behaviour	$1.31 \leq \alpha \leq 1.4$	1.35

zero then malicious or benign activity will not update trust value. The security level is controlled by β. β can have value from 0 to 5. The value of $\beta = 1$ is level 1 security. At this level all malicious activities are taken into account. The maximum allowed percentage change in trust value at this level is 20% as of level 0.

Assumption $\beta = 5$ is the maximum security level.

As the security level increases the punishment for a bad behaviour increases. When a node acts maliciously its neighbour isolate it from there route discovery. This isolation is not for indefinite time. After *ISOLATION_TIMEOUT* is over,isolated node is brought back into network with same trust value. ISOLATION_TIMEOUT is defined as in Equation 7

$$ISOLATION\_TIMEOUT = \alpha \times \beta^2 \times PATH\_DISCOVERY\_TIME^5 \quad (7)$$

The ISOLATION_TIMEOUT is directly proportional to behaviour of node. As the behaviour becomes bad, the node is out of routing for a longer time. ISOLATION_TIMEOUT increases significantly when the security level is increased. It is proportional to β^2, which makes the punishment harder. As the security level goes up it becomes difficult for the nodes to gain trust.

[5] 2800 ms, As defined in RFC 3561, Section 10

4.3 Path Selection

The path with the high trust value is selected. The overall trust is product of individual trust of the nodes in the path. The overall trust is calculated as per Equation 8

$$Route\ Trust \quad = \quad \prod_{i=source}^{destination} (Trust_{node\ i}^{node\ i+1}) \tag{8}$$

Where $Trust_{node\ i+1}^{node\ i}$ is trust value of node i on node i+1.

The Equation 8 controls the hop count of selected route. For example consider two routes are found. Route 1 has 3 intermediate nodes, and their trust value is 0.75, 0.75, 0.80. Route 2 has 6 intermediate nodes and their trust value is 0.80, 0.80, 0.80, 0.80, 0.80, 0.80. Although in Route 2 trust of individual node is higher than the trust value of the same in Route 1. However the hop count of Route 2 is 100% more than that of Route 1. The overall trust of Route 1 and 2 using Equation 8, is 0.45 and 0.26 respectively. Route 1 is better than Route 2 thus calculation of route trust using this equation gives shortest path with maximum security [9].

5 Experiment/Simulations

TBAODV is designed to isolate malicious node from participating in routing. To achieve this goal I have analysed various network scenarios. The network configuration is varied by changing the number of malicious nodes. The traffic model of the network is kept constant under all scenarios.

5.1 Scenario

The area chosen for network is 1 sq. km. It is selected based on metric presented in [10]. 50 nodes in my simulation model show benign behaviour. Upto 15 node can show non benign behaviour. These values will maintain node connectivity. The mobile nodes uses random waypoint mobility model. The pause time for any mobile node is 40 seconds. The power radius of node is 160 meters. A node can change neighbours when it has traversed 160 meters assuming other nodes are static, after every pause time. Average speed of node can be $\frac{160}{40} = 4$ m/s. To evenly distribute the nodes a node can have maximum of 4 neighbour nodes(including malicious and benign). It can only send data (or packets) to them. The nodes are moving at speed of 4m/s with power radius of 160m.They move in x-y plane only.

Scenario has been defined *by the number of malicious node* in network. I started with initial value of 0 and gradually increasing them to 15. A new node is assigned a trust value of τ. If a node shows malicious behaviour then it is being *isolated* from routing. The values of all the simulation parameter are defined in Table 3. Traffic model is CBR session. Two benign nodes are selected randomly, one of them acts as source and other as destination. The source node transmits 2 RREQ control packets per second.

Table 3. Simulation Variables

Variable	Value	Type
Area	$1Km^2$	Constant
Power Radius	160 meters	Constant
Nodes	50	Constant
Malicious Nodes	0 to 15	Variable
Traffic	CBR Session	
Mobility	Random	
Speed	4 m/s	Constant
Mobility Interval	40 Seconds	Constant
Packet Rate	2 Packets/second	Constant
Maximum Connections	4	Constant
Threshold Trust Value (τ)	0.65	Constant
Security Level(β)	1	Constant
χ	1.5	Constant

5.2 Node Model

The nodes were modelled as per specification given in RFC 3561. These nodes forward data and control packets to other nodes. Once benign node detects any malicious node within its power radius, it stops communicating to that node till ISOLATION_TIMEOUT is over. The non benign nodes were modelled such that they violate certain specifications defined in RFC 3561. Non benign behaviour is shown by following type of nodes.

- **Selfish Node**: They drop the control packet and participate in routing only when they want to send data.
- **Selfish Node**: The availability of these nodes are less than 99.999%.
- **RREQ Flooding Node**: These node flood the network with RREQ packets. They generate RREQ packet at higher rate than allowed for a node. These do not forward control packets.

Malicious nodes do not work in team. As each node has behaviour constant α and χ. The values of these constants are shown in Table 2 and 3. The selected values are not optimal for any network. I selected these values so that I can efficiently isolate the malicious nodes. Figure 1 shows the change in trust value for malicious node that floods the network with RREQ packets.

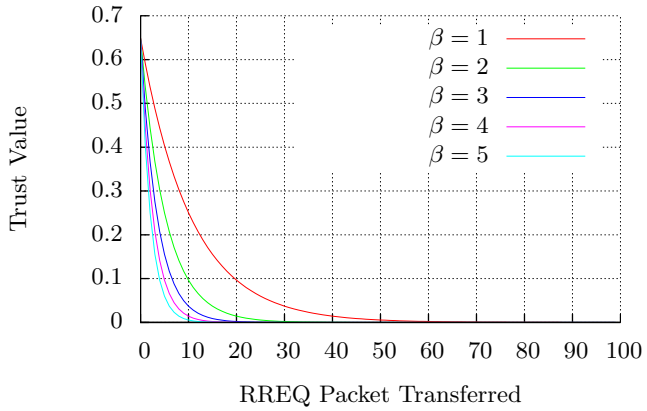

Fig. 1. Change in Trust for $\alpha = 1.05$ RREQ Flooding

In Figure 2 the change in trust value is shown for every successful RREQ transfer. In this figure trust of Node X on Node Y is shown. Where both the nodes are benign. Node Y forwards the packet sent by Node X correctly. So the Node X increases trust value for Node Y. The trust value is updated using function in Equation 4. The change in trust value is not same at different security level. For $\beta = 2$ the change in trust value for Node Y is less as compared for $\beta = 1$.

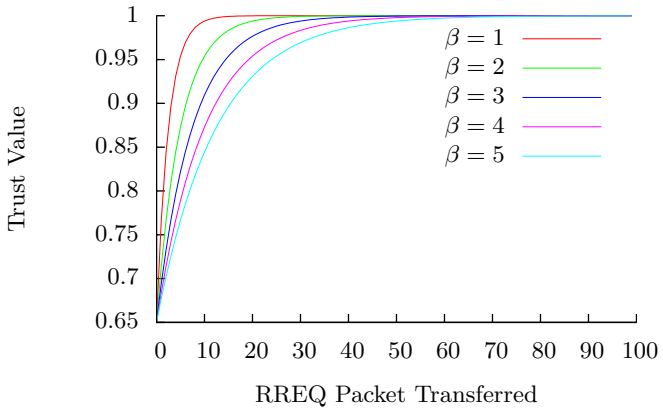

Fig. 2. Change in Trust Value (Benign Behaviour)

In Section 6.4 I have discussed about the trust value for various malicious nodes at different security level. For selected values of α in Table 2 the convergence of graph is faster to zero.

6 Results and Discussion

The performance of proposed protocol has been evaluated on two metric.

1. Routing Traffic.
2. Routes and Hop count.
3. Source to destination packet forwarding ratio (SDPF).

6.1 Routing Traffic

In the Figure 3 the source node sends first RREQ packet at 100ms to one of its neighbour. Then the neighbour forwards the packet to other nodes. The control traffic is generated and it grows until the destination is found. The increase in traffic is only due to RREQ packets. The RREQ Forwarded-AODV line corresponds to routing traffic generated by AODV while the RREQ Forwarded-TBAODV line corresponds to TBAODV. The number of RREQ packets generated in TBAODV is less than the packets generated in AODV. The Reduction in RREQ-TBAODV line shows the reduction in routing traffic when TBAODV was used. Figure 3 shows the number of RREQ and RREP generated for one route

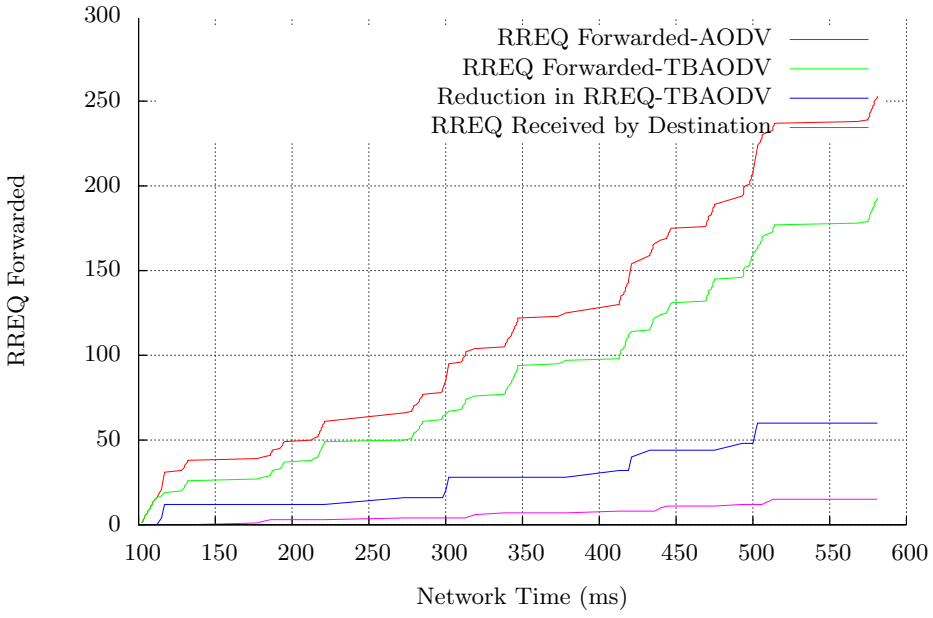

Fig. 3. Route Request Traffic, 6% Malicious Nodes

request. The total number of RREQ generated with AODV is 255 to discover a route. In response to that there are 15 RREQ received by destination node.

In the proposed protocol the number of RREQ generated is 20% less than the number of RREQ generated in AODV.

6.2 Route and Hop Count

Two benign nodes are randomly selected from simulation model having 20% malicious nodes, one is assigned as source and the other as destination. The source node initiates the process of route discovery. Figure 4 shows the trust value and hop count of all the routes that exists between the source and destination. There are 16 routes between them. First route has 26 hops and a trust value of 0.65. The intermediate nodes for this route are benign. Route 13 and 14 has the maximum trust value while route 15 and 19 are at second and third highest. According to proposed protocol Route 13 and 14 is most secure, but former has less hop count so Route 13 is best route for data transfer.

Route: Source Node → Intermediate Nodes → Destination Node. The trust value of route is calculated using equation 8.

Route 16 can also be considered as one of the most efficient routes. The trust value and hop count for this route is 1.4% and 5% less than the trust value of Route 13 respectively. TBAODV is designed for maximum security based on trust value so Route 13 is preferred.

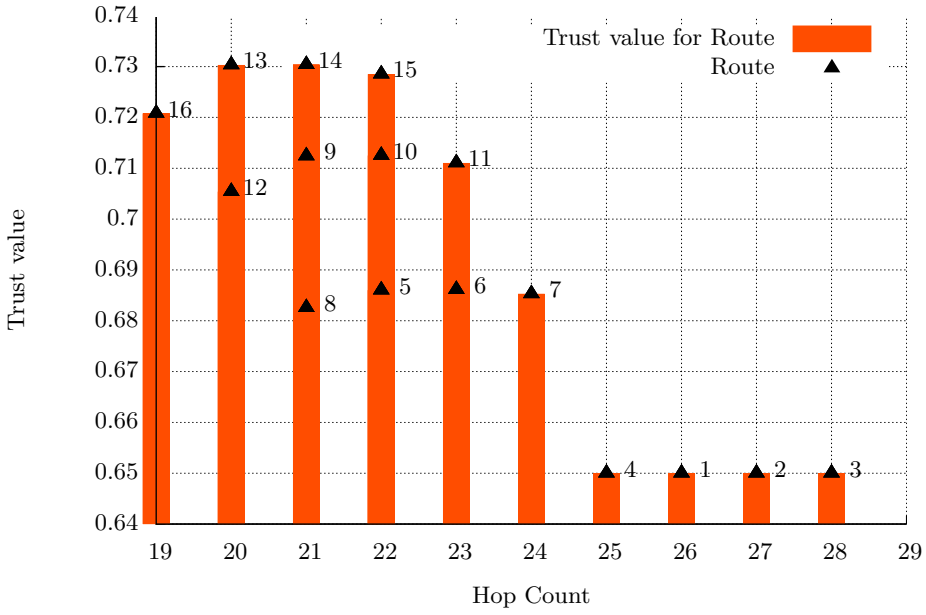

Fig. 4. Trust and hop count for each route found

6.3 SDPFR

It is the ratio between the number of RREQ packets forwarded during route discovery to the number of packets received by destination node.

$$SDPFR = \frac{\sum RREQ\ Forwarded}{\sum RREQ\ Received} \tag{9}$$

This ratio reflects the effect on packet loss. The lost packet covers all packets droped by malicious nodes only. In Figure 5 malicious nodes are randomly placed. I started simulation with zero malicious node in the network. In Figure 5 (SDPFR-AODV) the number of malicious node was increased from 0 to 15 as a consequence the SDPFR had increased from 8 to 17. This demonstrates malicious nodes had increased the routing overhead and packet loss.

In my proposed routing protocol, nodes discards the control packets sent by malicious node. Hence the routing overhead drops significantly. When the number of malicious node increases more number of routes is captured by the malicious node and more data packets is droped by them. The SDPFR has decreased significantly when trust was used as a routing metric. In Figure 5 (SDPFR-TBAODV) there is decrease in SDPFR. The control packets generated by malicious node is being discarded by the non malicious nodes. This reduces volume of routing traffic.The average SDPFR is calculated for control packet generated over 80 seconds. Since the nodes are mobile therefore mobility is also included.

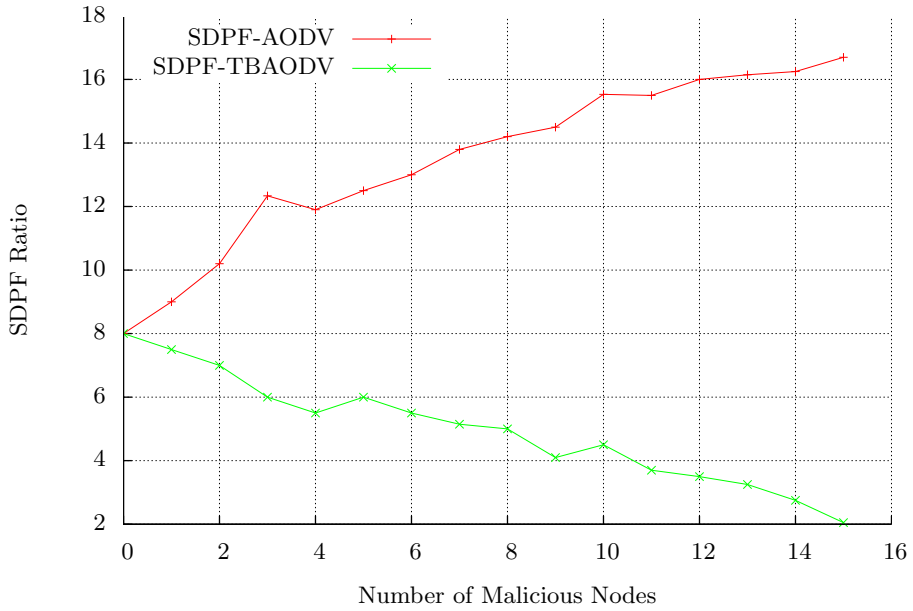

Fig. 5. Average SDPFR, $\beta = 1$, Constant Traffic Model

6.4 Change in Trust Values

Figure 2 demonstrates the change in trust value of benign node at different security level. As a node transmits a RREQ packet successfully, it's neighbour increases trust on it. Figure 6 shows the change in trust value for following behaviours.

- RREQ Flooding node
- unreliable behaviour.
- Selfish behaviour.
- Unexpected malicious behaviour.

The graph shows the change in trust values at different security level. The trust values converges to zero faster at maximum security level.

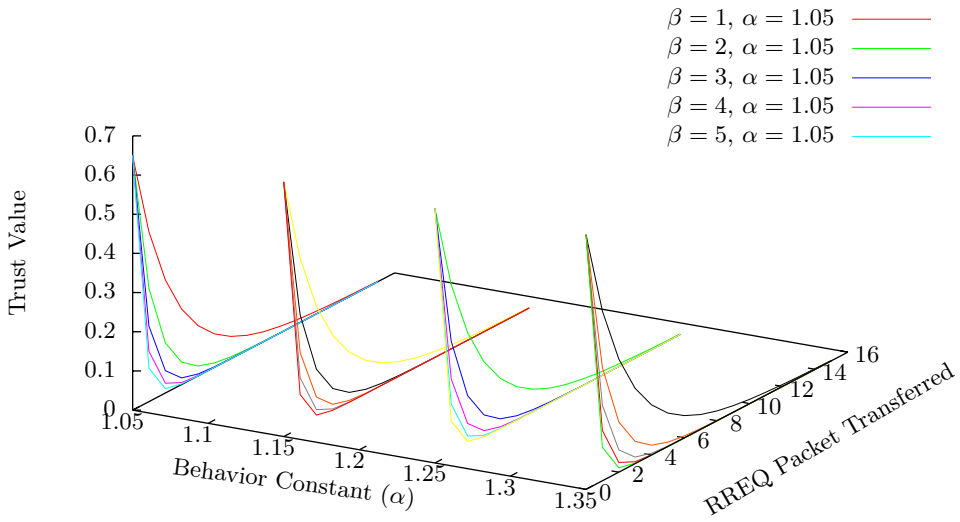

Fig. 6. Change in Trust for all α

7 Conclusion

A new protocol based on AODV is proposed to isolate malicious node from participating in routing. It calculates the trust for each node and makes sure the path is secure. I have simulated the protocol with upto 30% of malicious nodes and compared it with the performance of AODV based on routing overhead and

SDPFR. The results from simulation indicate that proposed protocol has less roting overhead and less normalised routing load in the presence of malicious node.

This paper discusses about detecting three behaviour. The values for behaviour constant is not suitable for all the network. These values are specific to my simulation. There is room for improvement for calculating behaviour constants.

References

1. Abolhasan, M., Wysocki, T., and Dutkiewicz, E., A review of routing protocols for mobile ad hoc networks, Elsevier, June 2003.
2. Blaze, M., Feigenbaum,J., and Lacy, J., Decentralised trust management. In Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 164-173, 1996.
3. Dahill,B., et al.,A Secure Protocol for Ad Hoc Networks, IEEE ICNP, 2002.
4. Falcone, R., and Castelfranchi, C., Social trust: A cognitive approach. In Trust and Deception in Virtual Societies, pp. 5590. Kluwer Academic Publishers, Dordrecht, 2001.
5. Ford, R., and Howard, M., Security in mobile ad-hoc Networks Published by the IEEE Computer society, 1540-7993/08, IEEE, IEEE Security & Privacy, 2008.
6. Gambetta, D., Can We Trust Trust? In Gambetta, D., editor, Trust: Making and Breaking Cooperative Relations, pages 213-238. Basil Blackwell. Oxford, 1990.
7. Hu, Y., C., Johnson, D., B., and Perrig, A., Ariadne: A secure On-Demand Routing Protocol for Ad-hoc Networks, in Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom), Atlanta, GA, September 2002.
8. Jsang, A.,Ismail, R., and Boyd, C.,A Survey of Trust and Reputation Systems for Online Service Provision, Decision Support Systems, Elsevier, 2007.
9. McGibney, J., and Botvich, D., Distributed Dynamic Protection of Services on Ad Hoc and Peer to Peer Networks, Proc. 7th IEEE International Workshop on IP Operations and Management (IPOM), San Jose, CA, USA, Lecture Notes in Computer Science (LNCS) 4786, pp 95-106, Springer, November 2007.
10. Lee,S.,J., Belding-Royer, E.M., Perkins, C.E., Scalability study of the ad hoc on-demand distance vector routing protocol, Int. J. Netw.Manage. 13 (2) (2003) 97–114.
11. McKnight, D.H., and Chervany, N.L., The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Research Center, 1996.
12. Papadimitratos, P., and Haas, Z., Secure Routing for Mobile Ad Hoc Networks, CNDS, 2002.
13. Perkins, C., Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003.
14. Rivest ,R.L., AND Lampson, B.,SDSIA simple distributed security infrastructure version 1.1, http://theory.lcs.mit.edu/ rivest/sdsi11.html, 1996.
15. Shanmugavel, S., Martin Leo Manickam, J., Fuzzy based trustes Ad-hoc On Demand Distance Vector Routing Protocol fro MANET, Third IEEE International Conference, WiMob, 2007.

16. Song, S., Hwang, K., and Zhou, R., University of Southern California, Trusted P2P Transactions with Fuzzy Reputation Aggregation, Published by the IEEE Computer Society, November - December 2005.
17. Stajano, F., and Anderson, R., The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, Springer, 1999.
18. Yi, S., Naldurg, P., and Kravets, R., A Security Aware Routing Protocol for Mobile Ad-hoc Networks, in Proceedings of the 6th World Multi-Conference on Semantics, Cybernetics asn Informatics (SCI), pp. 286-292, Orlando, FL, July 2002.
19. Zapata, M., and Asokan, N., Securing Ad Hoc Routing Protocols, ACM Wise, 2002.