Design of a Novel Trust Model and its Application in Trust based Routing to Defend against Dishonest Recommenders

Shirina Samreen
Research Scholar, Dept. of Computer Science
JNTUH College of Engineering
Kukatpally, Hyderabad, A.P., India

G.Narsimha, Ph.D
Associate Prof., Dept. of Computer Science
JNTUH College of Engineering
Nachupally, Kondagattu, Karimnagar, A.P., India

ABSTRACT
Trust management frameworks play a very important role in securing the mobile ad hoc networks against various insider attacks that could occur during data forwarding. The success of a trust management framework greatly depends upon the proper design of each of its major components including the direct trust computation component as well as the indirect trust computation component. Specifically, the indirect trust computation component should be robust to handle the dishonest recommendations. The current paper shows the application of a trust model involving a robust indirect trust computation component called as RecommFilter which has been proposed in our earlier work. It can overcome the various attacks caused by dishonest recommenders. The application involves the integration of the trust model with a routing protocol based upon a reliability measure called as Path Allegiance metric (PAM) which is a cumulative value obtained through the trust values of the on-path nodes upon each other. Experimental results show that the proposed scheme along with PAM routing protocol is robust to different dishonest recommendation attacks and accurate in the detection of dishonest recommenders.

General Terms
Mobile Ad hoc Networks, Trust Management framework, Uncertainty reasoning.

Keywords
Dempster Shafer Theory, Dishonest Recommenders, Slandering attack, Self-promoting attack, Collusion attack, Recommendation Filtering, Jousselmes distance, Path Allegiance Metric.

1. INTRODUCTION
Security in mobile ad hoc networks is quite challenging due to the inherent characteristics of dynamically changing topology, resource constraints, lack of physical security and infrastructure. To a large extent, the security needs of a MANET are addressed by the cryptographic measures which come under hard security measures but as the attackers become more and more challenging by exhibiting a legitimate behavior initially and then exhibit the malicious behavior, specifically the security issue at the data plane wherein the attackers may behave legitimately during the route establishment and then start exhibiting malicious behavior by either dropping the data packets or propagating false measurements, the hard security will not suffice and has to be integrated with trust based schemes that come under soft security measures [1]. The efficiency of a trust based framework depends upon its robustness to several attacks which can effect the trust evaluation itself. One of the most challenging attacks is due to the dishonest recommendations which have to be filtered out. A great deal of research has been done in dealing with dishonest recommendations [2-7]. Three different approaches can be employed to deal with dishonest recommenders according [4]: Majority rule based, Personal experience based and Service reputation based.

Dishonest recommendations attacks have been addressed in [4] which strives to overcome the drawbacks and improve the robustness by using a majority rule approach along with two additional novel mechanisms which help in the correction of false positives and false negatives. The scheme's limitations are addressed in the RecommFilter scheme [8]. A combination of majority rule based and personal experience based approaches is used along with a novel mechanism of precedence/priority based rules and a nearest neighbor clustering algorithm employing the Dempster Shafer Orthogonal sum[9][10] and Jousselmes distance [11]. The contributions of this work are as follows:

- Design of a novel uncertainty reasoning based trust model robust against dishonest recommenders and a dishonest recommenders filtering scheme called as RecommFilter which is used to refine the indirect trust value.
- Recommendation Trust Update module based upon a condition that the Jousselmes distance between recommended trust values of the current trust update period and the corresponding direct trust values obtained by the evaluating node in the next successive trust update period to be less than the maximum threshold.
- Design of a novel routing protocol called Path allegiance metric routing protocol (PAMRP) leveraging upon the proposed trust model.
- Analysis of the integrated functionality of the proposed trust model with RecommFilter scheme along with PAMRP in the presence of an attack model comprising of packet droppers and dishonest recommenders.

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 describes the trust model employed by the proposed scheme, section 4 describes the details of the RecommFilter scheme with the details of each of the modules involved, section 5 describes the Path Allegiance Metric routing protocol, section 6 describes performance analysis and section 7 presents the conclusion.

2. RELATED WORK

The attacks caused by dishonest recommendations form a major challenging issue when the security of a MANET is built upon a trust management framework employing the direct trust as well as indirect trust obtained through recommendations. A great deal of research has been done in the area but it becomes more challenging when the attackers exhibit more complicated malicious behaviors. According to [4], a classification of the schemes to address the problems of dishonest recommendations can be as follows: (1) Personal Experience based (2) Majority Rule based and (3) Service reputation based.

Personal experience based approaches [3] filter out those recommendations which deviate much from the opinion of the evaluating node. The main drawback of these approaches is that in a MANET environment a recommendation may represent the extent of interaction experience which the recommender had with the node being evaluated. This may vary significantly from the interaction experience of the evaluating node. Hence discarding the recommenders based upon its deviation from the personal experience may not result in a proper and accurate evaluation resulting in an increased number of false positives and false negatives.

In majority rule based schemes, opinions which match the majority are accepted as honest and the rest are treated as dishonest. A clustering based technique to filter out false recommendations and then apply the majority rule to choose the cluster with highest number of recommendations to compute the indirect trust was proposed by Yu et al. [5].

Service reputation based approaches assume that a node which had built a high reputation due to its service always provides honest recommendations. Such an approach was used by Zouridaki et al. [6] wherein the recommendations from highly reputed nodes are considered more trustworthy than the ones from low reputed nodes.

In view of the drawbacks of the above schemes, an approach called RecommVerifier was proposed which used the majority rule based approach along with two novel mechanisms of time verifying and proof verifying. The scheme works well in coping with dishonest recommendations but may become space intensive in case of large number of recommendations and also it uses a trust model based upon beta probability distribution which does not explicitly quantify uncertainty.

The proposed approach employs a trust model based upon Dempster Shafer theory [9] for the quantification of uncertainty so as to have accurate estimates of trust irrespective of the amount of evidence available. A novel feature of having a selection module to choose a fixed size subset of recommendations based upon precedence/priority based rules ensures that the approach does not incur storage overhead even in a densely populated network scenario where the number of received recommendations may be large.

3. TRUST MODEL

The trust formation is based upon the traditional Trust Management System (TMS) which exploits the Beta distribution, Beta (α, β) to compute the trust with respect the extent of cooperation extended for reliable data delivery where the variable α represents a measure of cooperative behavior and the variable β represents a measure of malicious behavior.

The proposed scheme uses an approach proposed in [10] leveraging on the Dempster-Shafer Theory for the quantification of the uncertainty involved. The variables (α, β) are mapped to the tuple (b, d, u) where b represents the belief metric in the cooperative behavior, d represents the disbelief metric in cooperative behavior, and u represents a measure of uncertainty satisfying b+d+u=1. The mappings are specified in the following equations:

$$b = \frac{\alpha}{\alpha+\beta} \times (1-u) \quad d = \frac{\beta}{\alpha+\beta} \times (1-u)$$

$$u = \frac{12 \times \alpha \times \beta}{(\alpha+\beta)^2 \times (1+\alpha+\beta)}$$

With the tuple (b, d, u) representing the trust components, the overall trust is computed as $T = b + \sigma \times u$ where the constant $\sigma = 0.5$. The periodic trust updates are represented by the following equations: $\alpha(t+1) = \alpha(t) \times \tau_p(t) + p$ and $\beta(t+1) = \beta(t) \times \tau_q(t) + q$ Where p and q represent a measure of cooperative and malicious behaviors respectively during the time period Δt, τ_p and τ_q represent a time-based aging factors to refresh the value of α and β respectively which are defined as follows:

$$\tau_p(t) = \gamma \times \frac{\alpha(t)}{\alpha(t)+1} \text{ and } \tau_q(t) = \mu \times \frac{\beta(t)}{\beta(t)+1}$$

Where γ and μ are constants (set to 0.4 and 0.6 respectively) The motivation behind considering the normalized value of $\alpha(t)$ and to $\beta(t)$ to compute $\tau_p(t)$ and $\tau_q(t)$ respectively is to obtain a quantitative measure of a nodes behavior so that the aging factors change dynamically. The value of $\mu > \gamma$ so that punishment factor for misbehavior is greater than the reward factor for good behavior. In other words, the weight given to the misbehavior in the past for computing the current value of β is greater than the weight given to the good behavior in the past for computing the current value of α.The values of belief, disbelief and uncertainty are updated with the update of α and β. The values of p and q are initialized to zero after the update of $\alpha(t+1)$ and $\beta(t+1)$ respectively.

4. RECOMMFILTER SCHEME

The indirect trust through recommendations is computed using the proposed scheme which includes the following functionalities: Recommendations Selection module, Recommendations Filtering module, Recommended / Indirect trust evaluation module and Recommendation trust update module.

Recommendations selection module generates a set of relatively credible recommendations from the set of one-hop neighbors of the subject node. A fixed number (denoted by R) of recommendations are selected. The recommenders are limited to one-hop neighbors so as to minimize the control overhead and avoid trust recycle recursion.

Indirect trust evaluation module performs the aggregation of recommendation trust values obtained from the set of recommendations which are produced as the outcome of Recommendation Selection Module followed by the Recommendations Filtering module. The detailed working of each of the four modules has been covered in our earlier work.

4.1 Recommendations Selection Module and Recommendations Filtering Module

At each trust update period, each node receives a set of recommendations from its one-hop neighborhood. The recommendation of some node i (recommendee) submitted by

some other node j (recommender) is nothing but the direct trust of node j upon node i. A subset of these recommendations is selected based upon certain rules and criteria to be satisfied by the recommenders. The recommendations selection module chooses a set of recommendations from the received ones based upon the recommenders which have to satisfy certain criteria. The recommenders which have submitted the recommendations are considered in the order of priority based upon precedence rules as detailed in our earlier work. Recommendations Filtering module aims to filter out certain recommendations from the recommendations obtained through the recommendations selection module based upon inconsistencies among the recommendations because of false/fake recommendations. It results in reducing the inaccuracy of the indirect trust by eliminating/reducing the impact of bad recommenders. The algorithm is based upon clustering similar to approach proposed by Yu et al. [4] wherein the recommendations with least distance/dissimilarity or maximum similarity are merged into one cluster. The details have been covered in our earlier work .

4.2 Algorithm for Recommendation Trust Update Module

The module deals with the update of recommendation trust based upon the distance between the indirect trust as provided by the recommender and the actual direct trust as computed by the evaluating node. Assuming that the current trust update period is t, the evaluating node considers the indirect trust provided by each of recommenders of the earlier trust update period denoted by t-1 and updates their recommendation trust.

The algorithm given below illustrates the computation of the variables α and β for the update of recommendation trust for each of the recommenders by the evaluating node X. The recommendation trust tuple (b, d, u) is updated periodically at each trust update period using the updated values of α and β in the same way as the trust update of direct forwarding trust as explained in section 3.

In the context of recommendation trust, a positive event is counted if the indirect trust value as recommended in the earlier round deviates from the corresponding direct trust value within a pre-defined threshold Θ also referred to as RECOMM_THRESH. If the deviation crosses the threshold, then a negative event is counted.

4.3 Recommended / Indirect trust evaluation module

The Indirect trust evaluation module has to generate a final indirect trust value through the recommendations obtained from the filtered out recommendations out of the selected recommenders. It combines the recommendations using the Dempsters rule of combination explained in section 4.2.2 to generate the final indirect trust.

4.4 Overall trust formation through the integration of direct trust and indirect trust

The synthesis of the overall trust using the direct trust and the recommended trust is done using the approach proposed in [10] which leverages on D-S theory. The belief, disbelief and uncertainty components of the synthesized overall trust are computed as follows:

$$b_{i,j}^{\ o} = \varphi_1 \times b_{i,j}^{\ D} + \varphi_2 \times b_{i,j}^{\ R}$$

$$d_{i,j}^{\ o} = \varphi_1 \times d_{i,j}^{\ D} + \varphi_2 \times d_{i,j}^{\ R}$$

$$u_{i,j}^{\ o} = 1 - b_{i,j}^{\ o} - d_{i,j}^{\ o}$$

Where

$$\varphi_1 = \frac{\gamma \times u_{i,j}^{\ R}}{(1-\gamma)\times u_{i,j}^{\ D} + \gamma \times u_{i,j}^{\ R} - 0.5 \times u_{i,j}^{\ D} \times u_{i,j}^{\ R}}$$

$$\varphi_2 = \frac{(1-\gamma)\times u_{i,j}^{\ R}}{(1-\gamma)\times u_{i,j}^{\ D} + \gamma \times u_{i,j}^{\ R} - 0.5 \times u_{i,j}^{\ D} \times u_{i,j}^{\ R}}$$

γ is known as nodes character factor, which derives the weight given to direct trust and recommended trust. A value greater than 0.5 indicates that direct trust is given more weight whereas a value less than 0.5 indicates that recommended trust is given more weight. The overall trust is computed (as mentioned earlier) as follows: $T_{i,j}^{\ o} = b_{i,j}^{\ o} + \sigma \times u_{i,j}^{\ o}$ where σ known as relative atomicity is set to 0.5

Algorithm to compute (α, β) for updating recommendation trust

Input:
S1: set of all nodes for which node X has direct trust in the current trust update period t
S2: set of all nodes for which node X received recommendations in trust update period t-1
S3 : S1 ∩ S2
S4: set of all recommenders in the trust update period t-1
P[NN]: array containing count of positive recommendation events in the current trust update period t
Q[NN]: array containing count of negative recommendation events in the current trust update period t
NN: total number of nodes in the network
T_i^k: trust of node k upon node i
Δ: Jousselmes distance between two bodies of evidence
Θ: small positive threshold representing the maximum acceptable deviation of the computed direct trust from the recommended indirect trust (set to 0.05)
Output: Updated values of α[NN] and β[NN]
For each node Z in set S4 do
    p[Z] = 0
    q[Z] = 0
    For each node Y in set S3 do
        If Z provided indirect trust update of node Y
            If $\Delta(T_Y^{\ X}, T_Y^{\ Z}) \leq \Theta$
                p[Z]++
            Else
                q[Z]++
    End For
    α[Z] = α[Z] +p[Z]
    β[Z] = β[Z] +q[Z]
End For

5. PATH ALLEGIANCE METRIC ROUTING PROTOCOL

The proposed security mechanism has been designed so as to form the most reliable route wherein the reliability is

quantified by a metric known as Path Allegiance Metric. The proposed trust management framework is based upon a subtle fact that the trust metric of some node i is not a global value but the individual perceptions/opinions of the other nodes upon node i. Each node updates the trust upon a neighbor node i based upon the direct observations as well as indirect recommendations. The reliable data delivery along a source to destination path depends upon the strength of belief each intermediate node has upon its immediate upstream and downstream nodes upon the path. In other words, it depends upon the reliability of the individual links wherein a link in the current context refers to the radio links or an association between two successive nodes i and i+1 on the path when they come in the communication range of each other. The following metrics are involved in the proposed security mechanism to assess the probability of reliable data delivery on a source to destination path.

Definition 1: (Link Reliability metric) Let two nodes i and j form a link on the source to destination path represented as <i, j>, $b_{i,j}{}^{O}$ represent the belief component in the overall trust of node i upon node j, $b_{j,i}{}^{O}$ represent the belief component in the overall trust of node j upon node i, then the link reliability metric of link <i, j> is defined as:

$$LR_{i,j} = \frac{b_{i,j}{}^{o} + b_{j,i}{}^{o}}{2}$$

Definition 2: (Source Link Reliability metric) Let <i, j>, represent a link on the path from source S to destination D. Then the source link reliability metric is defined as the average of the belief components of the source node's direct trust upon each of the nodes associated with the link.

$$SLR_{i,j} = \frac{b_{s,i}{}^{D} + b_{s,j}{}^{D}}{2}$$

Where $b_{S,i}{}^{D}$ represent the belief component in the direct trust of source node S upon node i, $b_{S,j}{}^{D}$ represent the belief component in the direct trust of source node S upon node j.

Definition 3: (Link Allegiance metric) Let <i, j>, represent a link on the path from source S to destination D. Then the link allegiance metric is defined as the average of link reliability and source link allegiance metric.

$$LA_{i,j} = \frac{LR_{i,j} + SLR_{i,j}}{2} \text{ or } LA_{i,j} = \frac{b_{i,j}{}^{o} + b_{j,i}{}^{o} + b_{s,i}{}^{D} + b_{s,j}{}^{D}}{4}$$

Link Allegiance metric represents a measure of the reliability of the link with respect to its participation in the data transmission on a particular source to destination by taking into consideration the opinion of the source upon each of nodes associated with the two ends of the link along with link reliability expressed through the trust each end of the link has upon the other.

Definition 4: (Path Allegiance metric) Let the path from source S to destination D be represented as (S, 1, 2, 3,……., k, D).Then the path allegiance metric is defined as follows:

$$PAM_{S,D} = \underbrace{b_{s,1}{}^{o}}_{\substack{\text{one–way}\\ \text{belief of}\\ \text{first link}}} \times \underbrace{LA_{1,2} \times LA_{2,3} \times \cdots\cdots \times LA_{k-1,k}}_{\substack{\text{Link allegiance metrics of successive links}\\ \text{except first and last links}}} \times \underbrace{b_{D,k}{}^{o}}_{\substack{\text{one-way}\\ \text{belief of}\\ \text{last link}}}$$

Path allegiance metric is a quantitative measure of the commitment of each of the intermediate nodes towards the common goal of reliable data delivery along the chosen source to destination path. Hence the path allegiance metric is defined as the product of allegiance metrics of each of the successive links on the source to destination path except the first and the last links and the one-way belief components of the first and the last link.

The routing protocol obtains all possible trusted routes from source to destination which are sorted based upon the decreasing order of path allegiance metric and the path with highest PAM is used for data transmission. The available list of routes can be utilized in case of failure of an existing route thereby reducing the route formation delay. Fig. 1 below shows the formats of the various control packets involved during the working of the PAMRP.

5.1 Route Establishment

The procedure of establishment of a route from a source node to a destination node is as follows:

Step 1: When the source node S has to perform data transmission to a destination node D, it looks up in its routing table for the existence of a valid route.

Step 2: If there is a valid routing table entry in the routing table go to Step 4, else go to Step 3.

Step 3: If there are any unexpired valid routes in the route cache, select the route with highest Path allegiance Metric and go to Step 5, else go to Step 6.

Step 4: Perform the data transmission along the route. Go to Step 7.

Step 5: The source node S performs route setup by the unicast of RTSET packet along the selected route and sets a timer to wait for the reception of RTSET packet from the destination D. Upon the expiry of the timer, checks whether RTSET packet received from D. If yes goto step 4, else goto step 3.

Step 6: Perform a fresh route discovery through the broadcast of RREQ packet .

Step 7: Stop.

5.2 Route Discovery

The source node S broadcasts RREQ packet and each node maintains a monotonically increasing counter called as broadcast ID which is incremented whenever the source issues an RREQ. The source node also sets a timer for each broadcast ID to a fixed duration within which it has to receive the RREP packets for all possible paths. Upon the expiry of the timer, it selects a path from the route cache with the highest Path Allegiance Metric value using the RTSET packet. The unicast of RTSET packet along the S to D path followed by the unicast of RTSET packet along the D to S path results in the bi-directional update of the routing table entries of the intermediate nodes involved on the S to D path. The following pseudo-code describes the processing done by a node upon the reception of RREQ and RREP packets.

5.2.1 Reception of RREQ packet

Step 1: When a node x receives an RREQ from a node y, it first checks whether the destination address field consists of its own identifier. If yes, goto step 6 else goto step 2.

Step 2: It first checks whether the accumulated path field already consists of its own identifier x, if yes the RREQ is discarded as it involves a loop in the route. Otherwise goto step 3.

Step 3: The accumulated path is checked to see if it involves any useless round about path: If the length of the accumulated path is l and if any of the neighbors of node x are present at any position k such that k<l, then the accumulated path is pruned from position k+1 to l since the path segment comes under a round about path. The accumulated path field is updated to comprise the path segment from position 1 to k.

Step 4: The node x checks the disbelief component of its trust upon the sender node y, if it is greater than DISBELIEF_THRESH (0.4), then RREQ is discarded since the node x does not trust its upstream node. Otherwise goto step 5.

Step 5: Node x appends its identifier in the accumulated path field of RREQ and checks whether the belief component of its direct trust upon sender node y $b_{x,y}{}^{D}$ is greater than 0.5. If yes it appends $b_{x,y}{}^{D}$ in the upstream trust field of the RREQ, else it appends $b_{x,y}{}^{O}$ in the upstream trust field of the RREQ where $b_{x,y}{}^{O}$ represents the belief component of the overall trust upon node y by considering the indirect trust obtained through recommendations using the RecommFilter. Then it further broadcasts it. Go to step 1.

Step 6: The destination node x checks whether the RREQ packet with the given broadcast ID is the first one to arrive. If yes, it sets a timer and starts waiting. Otherwise it checks whether the timer has already expired which causes a discard of the RREQ packet, otherwise goto step 7.

Step 7: The destination node x extracts the upstream trust field and the accumulated path field from the RREQ and stores in its route cache. It checks the disbelief component of its trust upon the sender node y, if it is greater than DISBELIEF_THRESH (0.4), then RREQ packet is discarded since the node x does not trust its upstream node. Otherwise goto step 8.

Step 8: Checks whether the belief component of its direct trust upon sender node y, $b_{x,y}{}^{D}$ is greater than 0.5. If yes it appends $b_{x,y}{}^{D}$ in the upstream trust field of the RREQ, else it appends $b_{x,y}{}^{O}$ in the upstream trust field of the RREQ where $b_{x,y}{}^{O}$ represents the belief component of the overall trust upon node y by considering the indirect trust obtained through recommendations using the RecommFilter.

Step 9: It then creates an RREP packet, copies the upstream trust field and the accumulated path field into the RREP packet and discards the RREQ packet. It unicasts the RREP packet along the path specified in the accumulated path field.

Step 10: Stop.

u_int8_t rq_type; // Packet Type
u_int32_t rq_bcast_id; // Broadcast ID
nsaddr_t rq_dst; // Destination IP Address
nsaddr_t rq_src; // Source IP Address
nsaddr_t path[NETWORK_DIAMETER];
float upstream_trust[NETWORK_DIAMETER];

(a) RREQ packet header format

u_int8_t rq_type; // Packet Type
u_int32_t rq_bcast_id; // Broadcast ID
nsaddr_t rq_dst; // Destination IP Address
nsaddr_t rq_src; // Source IP Address
nsaddr_t *path;
float *upstream_trust;
float *downstream_trust;

(b) RREP packet header format

u_int8_t hello_type; // Packet Type
nsaddr_t *node_id; //list of nodes with trust updates
float *belief;
float *disbelief;
float *uncertainty;

(c) HELLO packet header format

u_int8_t rtset_type; // Packet Type
nsaddr_t *src;
nsaddr_t *dst;
bool reply_bit; // 0 if sent by D and 1 if sent by S
nsaddr_t path[NETWORK_DIAMETER];

(d) RTSET Packet header format

Fig.1. Formats of the control packets used in PAMRP

5.2.2 Reception of RREP packet

Step 1: When a node x receives an RREP from a node y, it first checks whether the disbelief component of its trust upon the sender node y, is greater than DISBELIEF_THRESH (0.4), then RREP is discarded since the node x does not trust its downstream node. Otherwise goto step 2.

Step 2: It checks whether the source address field consists of its own identifier. If yes, go to step 4 else goto step 3.

Step 3: Checks whether the belief component of its direct trust upon sender node y, $b_{x,y}^{D}$ is greater than 0.5. If yes, it appends $b_{x,y}^{D}$ in the downstream trust field of the RREP else it appends $b_{x,y}^{O}$ in the downstream trust field of the RREP which represents the belief component of the overall trust upon node y by considering the indirect trust obtained through recommendations using the RecommFilter. Then it further unicasts the RREP packet along the path. Goto step 5.

Step 4: The Source node checks whether the timer corresponding to the broadcast ID within the RREP has already expired. If yes, it discards the RREP packet. Otherwise, it extracts the upstream trust field, downstream trust field, accumulated path, and computes the Path Allegiance Metric (PAM) and stores the path and the corresponding PAM in its route cache.

Step 5: Stop.

5.2.3 Reception of RTSET packet

Step 1: When a node x receives an RTSET packet from a node y, it first checks whether the destination field matches its own identifier. If yes, goto step 2 else goto step 4.

Step 2: It checks whether the reply bit is on in the RTSET packet (indicating that the destination node D in the packet has to send back an RTSET packet to the source node S) , if yes goto step 4, else goto step 3.

Step 3: If reply bit is off in the RTSET packet (indicating that the source node S has received the reply RTSET from the destination node D), S discards the RTSET packet and starts the data transmission along the path.

Step 4: The destination D extracts the path field to update the routing table entry with the path to reach S, creates a new RTSET packet with the source address field having its own address, the destination address is set to S, the path field is set to the reverse of the path obtained from the RTSET packet sent by S, the reply bit is off and unicasts the packet along the path towards S. Goto step 5.

Step 4: The path field in the RTSET packet is used to update the routing table entry to reach the destination and the packet is further unicast according to the specified path. Goto step 5.

Step 5: Stop.

5.3 Recommendations Propagation

The proposed routing protocol utilizes an approach for neighborhood discovery similar to the used by AODV. Periodically, each node sends a HELLO packet which serves the dual purpose of neighborhood discovery as well as indirect trust propagation. Each node i considers its own direct trust updates upon each of the other nodes and incorporates it the HELLO packet which is broadcast to its one-hop neighborhood. Hence each node receives recommendations upon other nodes from its one-hop neighborhood (which acts as the set of recommenders). The received recommendations are processed through the RecommFilter scheme described in our earlier work to obtain a refined indirect trust value for each of the other nodes even in the presence of dishonest recommenders.

6. PERFORMANCE EVALUATION

The simulation experiments of the RecommFilter scheme are carried out through network simulator 2 using the proposed PAM routing protocol. The trust model is based upon Dempster Shafer theory of evidence as explained above in section 3. The performance of the proposed scheme is compared with Whitby's filtering scheme(WFS) [2] (based on majority rule), RecommVerifier(RV) [4] and E-Hermes(EH) [7] (based on personal experience).

In the simulation experiments, we consider the following attacks launched by dishonest recommenders. ***Slandering attack*** involves badmouthing or providing fake negative recommendations so as to lower the overall trust of the target node. ***Self-Promoting attack*** involves providing unfairly positive recommendations upon a target node so as increase its overall trust. ***Collusion attack*** occurs when multiple malicious nodes collude to work towards their selfish goals. Non-malicious nodes are assumed to forward 100% of the data packets whereas malicious nodes forward 20% of the data packets. The focus of the paper is dishonest recommendation problem hence the malicious packet droppers are fixed to 20% whereas the dishonest recommenders are varied from 0% to 90%.

The default values of the parameters for the simulation are listed in Table 1. The performance of the proposed security scheme is analyzed with respect to a significant varying parameter which is the percentage of dishonest recommenders.

Table 1. Experimental Parameters

Parameter	Value
Coverage area	800m x 800m
Number of nodes	50
Speed	0 to 50m/s
% Malicious nodes	20%
% Dishonest recommenders	Varied from 10% to 90%
Trust Update Period	50 s
Transmission Range	150 m
Simulation time	1000 s
Mobility model	Random Way Point
Traffic type	UDP-CBR(Constant Bit Rate)
Packet Size	512 bytes
Pause time	1 s

m=meter s=second

Firstly, the performance of the proposed RecommFilter scheme is analyzed in the form of a measure of the percentage of false positives and false negatives. As described, the proposed scheme does not merely depend upon the majority rule approach through the Recommendations Filtering module but utilizes the Recommendation Trust Update module which enables the Recommendation Selection module to filter out dishonest recommendations thereby providing a refinement to filtering module. The metrics used are the proportion of false positives proportion and the false negatives proportion (FPP and FNP respectively). ***False Positives Proportion*** is defined as the percentage of honest recommendations which are

wrongly detected as dishonest ones. ***False Negatives Proportion*** is defined as the percentage of dishonest recommendations which are wrongly detected as honest ones. The change in FPP and FNP with the passage of time is used to study the efficiency of the proposed scheme. In all the experiments, it can be observed that as time passes and the number of trust update periods increases, the results appear to be more refined, but the extent of refinement and the speed of convergence to nearest ideal result varies for different experiments.

Fig. 2 shows the FPP and FNP for the collusion attack, considering the percentage of dishonest recommenders to be 80% and 40%. It can be observed that the false positive proportion and false negative proportion decreases with time as the number of trust update periods increase. When the number of dishonest recommenders is fixed to 80%, at the time instant 900 seconds FPP and FNP are 10% and 5% respectively. In Fig. 1, it can also be observed that, the decrease in the FPP and FNP within a period of 800 seconds is 78% and 80% respectively. With RTU module, the true nature of more and more dishonest recommenders is revealed with time and hence the FPP and FNP also decrease drastically with time. When the percentage of dishonest recommenders is 40%, the FPP and FNP are much lesser when compared to the FPP and FNP with 80% dishonest recommenders.

Secondly, the performance of the proposed RecommFilter scheme in conjunction with the proposed PAM routing protocol is analyzed in the form of packet delivery fraction (PDF) and routing overhead (ROV) obtained with different values of RECOMM_THRESH (represented by the symbol Δ). The significance of the parameter Δ which is used to update the recommendation trust can be interpreted with the analysis. In Fig. 3, the packet delivery fraction achieved is shown with respect to disbelief threshold (represented by the symbol δ) for different values of Δ. For all values of Δ, a common observation is when δ is 0.1, the number of false positives with respect to packet droppers is highest and many good nodes are also avoided during route formation resulting in a greater route formation delay thereby resulting in a reduced PDF. When δ=0.3, PDF improves since the number of false positives decrease. For all values greater than 0.3 for δ, as the value of δ increases, the PDF decreases since the number of false negatives increase because of a liberal disbelief threshold.

In Fig. 4, the routing overhead incurred is shown with respect to disbelief threshold (represented by the symbol δ) for different values of Δ. For all values of Δ, a common observation is when δ is 0.1, the number of false positives with respect to packet droppers is highest and many good nodes are also avoided during route formation resulting in a greater route formation delay with a reduced routing overhead. When δ=0.3, the number of false positives decrease and the routing overhead increases. For all values greater than 0.3 for δ, as the value of δ decreases, the routing overhead also decreases due to an increase in the number of false negatives. But the decrease in routing overhead for each value of δ is quite small because, even though the number of false negatives increases due to a liberal disbelief threshold, the malicious nodes which are not detected during the route formation phase will be detected during the data transmission phase resulting in the propagation of RERR packets thereby adding to the routing overhead.

The value of Δ decides the amount of acceptable deviation in the recommended trust value in a trust update period and the corresponding direct trust value in the successive trust update period based on which the update of recommendation trust occurs. The values of Δ considered for the experimental analysis are 0.1, 0.15, 0.2 and 0.25. A very small value of Δ like 0.1 results in increased false positives with respect to dishonest recommenders which means that the number of recommenders reduce since many honest recommenders are wrongly detected as dishonest thereby resulting in inaccurate overall trust since most of the recommenders will be treated as dishonest thereby resulting in a reduced PDF of 80.2%. With respect to ROV, as can be observed in Fig.3, the average ROV is higher 0.322 since inaccurate trust value during the route formation may cause many malicious nodes which go undetected during route formation are detected during data transmission resulting in the propagation of RERR packets which adds to ROV. The value of 0.15 for Δ is ideal since it reduces the number of false positives and false negatives with respect to dishonest recommenders which results in a more accurate trust computation and hence increased PDF of 85.3% and reduced ROV of 0.274. When the value of Δ is higher like 0.2 and 0.25, the number of false negatives increase which means that many dishonest recommenders are treated as honest thereby resulting in an incorrect indirect trust value which effects the computation of overall trust thereby resulting in a reduced PDF 77.96% and decreased ROV 0.342.

The performance of RecommFilter in filtering out dishonest recommenders is analyzed using a metric called as trust convergence rate. ***Trust convergence rate*** is defined as the speed with which the trust computed using all the received recommendations gets closer to the actual trust metric representing the original nature of a node as malicious or non-malicious. The efficiency of the proposed RecommFilter scheme is analyzed by comparing it with two other schemes: the RecommVerifier Scheme [4] and the E-Hermes scheme [7]. The trust convergence rate is studied in two scenarios involving a slandering attack and self-promoting attack considering 80% dishonest recommenders. It can be observed that, the computed trust of a good node converges at 600 seconds after which the computed trust remains constant with time. Fig.5 shows the comparative analysis wherein the proposed RecommFilter scheme outperforms all the remaining two schemes. The convergence of trust using the RecommFilter scheme is closest to the actual trust metric reflecting the true nature of the node. In case of RecommVerifier scheme, even though it uses two novel schemes for refining the results of the detection of dishonest recommenders, since the trust model is based upon Bayesian inference, the trust computation may not be accurate enough compared to the trust model based upon Dempsters Shafer Theory since it includes the quantification of uncertainty. The E-Hermes scheme based upon the personal experience based approach performs lesser than the RecommVerifier as it discards all the recommendations which are not consistent with its own but the dynamic nature of a MANET may result in the evaluating node's interaction experience being insufficient in reflecting the true nature of a node thereby resulting in a slow convergence rate.

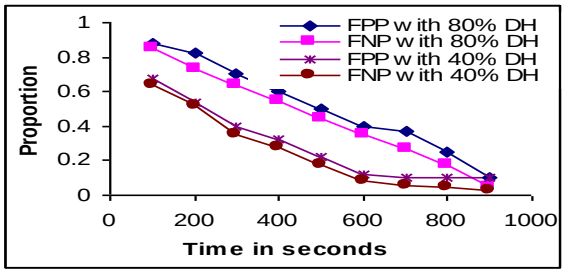

Fig.2: False Positive Proportion and False Negative Proportion for Collusion Attack

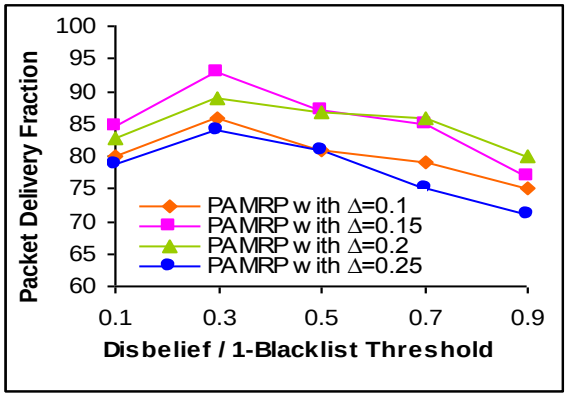

Fig.3: Packet Delivery Fraction with varying disbelief threshold and varying RECOMM_THRESH

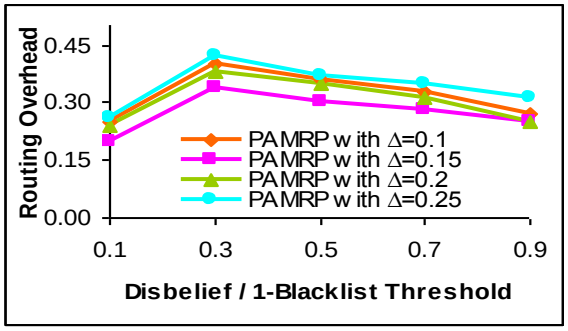

Fig.4: Routing Overhead with varying disbelief threshold and varying RECOMM_THRESH

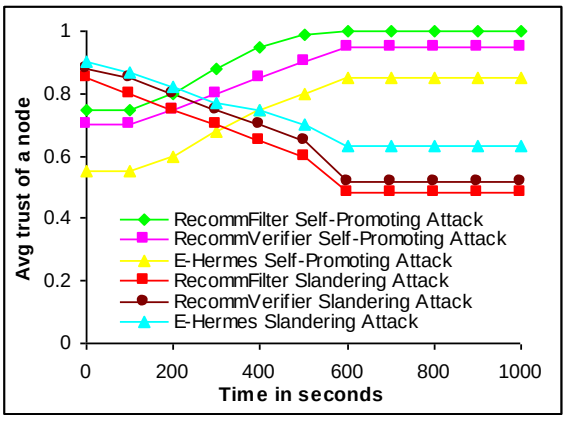

Fig.5: Trust Convergence rate

7. CONCLUSION

The novelty of the proposed RecommFilter scheme lies in the usage of Jousselmes distance to filter the recommendations. The trust model employs the Dempster Shafer Theory for quantifying uncertainty which is most appropriate in a dynamically changing environment of MANET. As far as we know, this work is the first one to utilize an opinion similarity measure through Jousselmes distance for filtering out the dishonest recommendations. The proposed scheme tries to overcome the limitations of the existing recommendation filtering defense schemes by employing a combination of multiple approaches including the majority rule based and the personal experience based along with a metric known as similarity index. The simulations experiments show that the proposed trust model incorporating the RecommFilter scheme along with the PAM routing protocol works efficiently even in the presence of 80% dishonest recommenders.

8. REFERENCES

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst., vol. 43, no. 2, pp. 618–644, 2007

[2] A. Whitby, A. Josang, J. Indulska, Filtering out unfair ratings in bayesian reputation systems, in: Proceedings of the Third International Joint Conference on Autonomous Agents and Multi Agent Systems, 2004, pp. 106–117.

[3] S. Buchegger, J.-Y. L. Boudec, A robust reputation system for p2p and mobile ad-hoc networks, in: Proceedings of the 2nd Workshop on Economics of Peer-to-Peer Systems, 2004, pp. 1–6.

[4] S. Chen, Y. Zhang, Q. Liu, and J. Feng, "Dealing with dishonest recommendation: The trials in reputation management court," Ad Hoc Networks, pp. 1603-1618, 2012

[5] H. Yu, S. Liu, A. C. Kot, C. Miao, and C. Leung, "Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks," in Proc. 13th IEEE Int. Conf. Commun. Technol., pp. 1-6, Sep. 2011

[6] C. Zouridaki et al., "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs," Proc. 3rd ACM Wksp. Sec. Ad Hoc and Sensor Networks, Alexandria, VA, Nov. 7, 2005

[7] C. Zouridaki, B.L. Mark, M. Hejmo, R.K. Thomas, E-Hermes: a robust cooperative trust establishment scheme for mobile ad hoc networks, Ad hoc Networks 7 (2009) 1156–1168.

[8] Shirina Samreen, Dr.G.Narsimha, "Dynamically Adaptive Recommender Filtering Scheme to defend against Dishonest Recommenders in a MANET", International Journal of Science and Research, Vol.4, Issue 5, pp.388-398, 2015

[9] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, 1976

[10] F. Li, J. Wu, Mobility reduces uncertainty in MANETs, in: Proceedings of INFOCOM'07, 2007, pp. 1946–1954

[11] A. L. Jousselme, D. Grenier, and E. Bosse, "A new distance between two bodies of evidence," Information Fusion, vol. 2, no. 2, pp. 91–101, 2001