International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Dynamically Adaptive Recommender Filtering Scheme to Defend against Dishonest Recommenders in a MANET

Shirina Samreen[1], Dr. G. Narsimha[2]

[1]Research Scholar, Dept. of CSE, JNTUH, Kukatpally, Hyderabad, Telengana, India

[2]Associate Professor, Dept. of CSE, JNTUHCEJ, Nachupally, Karimnagar,Telengana, 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. In this paper, we propose a novel and effective scheme used to design a robust indirect trust computation component called as RecommFilter which can overcome the various attacks caused by dishonest recommendations. Four components namely, Recommendation Selection module, Recommendation Filtering module, Recommendation Evaluation module and Recommendation Trust Update module work in close collaboration to filter out the dishonest recommendations and protect against slandering attacks, bad-mouthing attacks as well as collusive attacks. The novelty of the proposed scheme is that it employs a combination of personal experience based approach as well as majority rule based approach wherein the Selection Module using the personal experiences involves a multi-dimensional trust represented using the Dempster Shafer Theory of evidences and the filtering module using the majority rule involves a clustering based approach performed through an opinion similarity measure computed using the Jousselmes distance between two basic probability assignments (bpa). Experimental results show that the proposed scheme is robust to different dishonest recommendation attacks and accurate in the detection of dishonest recommenders.***

Keywords: Mobile Ad hoc Networks, Trust Management framework, Dempster Shafer Theory, Dishonest Recommenders, Slandering attack, Self-promoting attack, Collusion attack, Recommendation Filtering, Jousselmes distance, Opinion Similarity measure.

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. The most challenging of the 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 [4-10].

Most of the existing trust management frameworks deal with the problem of fake recommendations using three different approaches according to [11]: Majority rule based [6-7], Personal experience based [4],[8-9] and Service reputation based [5] and [10].

Keeping in mind the drawbacks of the above schemes, a new approach to deal with attacks caused due to dishonest recommendations, has been proposed in [11] 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 proposed approach is designed to incorporate most of the features of the scheme in [11] and overcome the limitations. It uses a combination of majority rule based and personal experience based approaches and incorporates a novel mechanism of precedence/priority based rules and a nearest neighbor clustering algorithm employing the Jousselmes distance and Dempster Shafer Orthogonal sum. Our contributions in the proposed approach are as follows:

- Even in the case of reception of large number of recommendations, it employs certain precedence/priority based rules for selecting only a fixed number of recommendations K which are provided as input to the filtering module.
- The precedence/priority rules make use of a multi-dimensional trust including the recommendation trust and forwarding trust. Apart from this, a metric to weigh the credibility of a recommender is the similarity index computed by generating the Jousselmes distance [20] between the corresponding direct trust of the evaluating node and the recommender node.
- Recommendation Filtering module which involves a

nearest neighbor clustering algorithm which selects a subset of recommendations using the majority rule approach. The distance between the clusters is evaluated using Jousselmes distance between bodies of evidence.

- A novel 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.

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 describes the attack model, section 4 describes the trust model employed by the proposed scheme, section 5 describes the details of the proposed RecommFilter scheme with the details of each of the modules involved, section 6 describes the 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 [2], [3] 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 [11], a classification of the schemes to address the problems of dishonest recommendations can be as follows: (1) Majority Rule based (2) Personal Experience based and (3) Service reputation based.
In majority rule based schemes [6-7], 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.[12].

Personal experience based approaches [8-9] 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.

Service reputation based approaches [10][14] 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.[14] 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 in [11] 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 the uncertainty.

The proposed approach employs a trust model based upon Dempster Shafer theory [18] 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. The Attack Model

A trust model based upon the usage of direct trust through first hand observations as well as the indirect trust through second hand observations has the dishonest recommendations as one of its most challenging issues. According to [12], two possible attacks which have been identified are as follows:

Slandering Attack: It involves badmouthing or providing fake negative recommendations so as to lower the overall trust of the target node.

Self-Promoting Attack: It involves providing unfairly positive recommendations upon a target node so as increase its overall trust. It is also called as ballot stuffing attack.

Apart from the two basic forms of attacks, attack in another complicated form may arise when multiple malicious nodes collude to work towards their selfish goals.

A slandering / self promoting attack performed by an individual node may be addressed well with majority rule based approach since the dishonest recommender is a minority. When the nodes collude, the majority rule based approach may not suffice since the number of dishonest recommendations may increase. Hence, the results of filtering module may involve false positives and false negatives which are corrected by the recommendation trust update module.

The recommendation trust update module should adapt itself to the dynamically changing behaviors of the dishonest recommenders which may adopt an intelligent strategy of initially providing the honest recommendations and then switching into the dishonest mode so as to confuse the defense scheme. Hence an adaptive fading factor is used for the recommendation trust update.

4. Trust model for the RecommFilter scheme

4.1 Trust Representation

The direct trust of a subject node i upon some other node j is

computed by taking into consideration, the extent of cooperation extended by node j during the route establishment and the data transmission. 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.

Most traditional TMS use the Bayesian theorem [16] which provides a statistical inference in which evidence is used to update the probability of a hypothesis being true. The theorem uses the beta probability distribution Beta (α, β) since it needs only two parameters which get updated as new evidence is collected. In practice, within the environment of a MANET, the usage of Bayesian inference may not provide accurate results when used for computing the nodes trust with respect to the cooperative behavior since the lack of evidence about an event is treated as a negative evidence. Specifically, in MANET for example a value 0 may indicate no past interactions or all malicious interactions between two nodes. In Bayesian inference, a node can hold either a positive or negative attitude towards an event, for example if a node A has observed that node B exhibited malicious behavior 10% of time, then node A assumes that node B is non-malicious with 90% probability but it may be very much possible that for the remaining 90% of time (other than malicious behavior), node A might not have observed some of the behavior because of some environmental reasons like node mobility, limited radio range and noise in the channel. Hence Bayesian inference may result in incorrect estimates of behavior in a MANET mainly because of the uncertainty involved as a node may not be able to observe its neighbors behavior completely and hence the initial observations involve a lot of uncertainty.

The inherent characteristics of the MANET require an approach where the uncertainty about an event is also properly represented. Dempster Shafer theory (DST) is more appropriate when there is uncertainty or no prior knowledge about an event. In DST, lack of evidence about an event is not considered as negative evidence and a node may hold a supportive or uncertain attitude towards an event. For example if a node observed 10% of malicious behavior, it cannot straightaway conclude 90% good behavior but rather it concludes 10% malicious behavior and 90% uncertainty.

The proposed scheme uses an approach proposed in [17] leveraging on the Dempster-Shafer Theory [18] 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 $T = b + \sigma \times u$ following the literature [19].

Specifically, $\vec{T}_{i,j}^{\,D}$ represents the direct trust of node i upon node j consisting of the tuple $\left(b_{i,j}^{\,D}, d_{i,j}^{\,D}, u_{i,j}^{\,D}\right)$ representing the belief, disbelief and uncertainty components. The constant σ is called as relative atomicity based on the principle of insufficient reasoning wherein the uncertainty of n atomic states is split equally among n states. Hence the uncertainty of the two states of good forwarding and bad forwarding is split equally without any bias on a particular state so that $\sigma = 0.5$.Trust in any open network has the property of aging with time. In other words, irrespective of whether any interaction occurs between two nodes or not, trust fades away with time. Hence time based aging factor has to incorporated in the trust framework. At periodic intervals of time period Δt, trust has to be updated through the updates of **α** and **β** by adding the measure of cooperative behaviors and malicious behaviors within the period Δt to the old values aged by a factor of **τ**.

The periodic trust updates are represented by the following equations:

$$\alpha(t+1) = \alpha(t) \times \tau_p(t) + p$$

$$\beta(t+1) = \beta(t) \times \tau_q(t) + q$$

Where p and q represent a measure of cooperative and malicious behaviors respectively during the time period Δt, τ_p represents a time-based aging factor for refreshing the value of **α** which is defined as follows:

$\tau_p(t) = \gamma \times \frac{\alpha(t)}{\alpha(t)+1}$ Where γ is constant (set to 0.4)

The motivation behind considering the normalized value of $\alpha(t)$ to compute $\tau_p(t)$ is to obtain a quantitative measure of a nodes behavior so that the aging factor $\tau_p(t)$ changes dynamically. τ_q represents a time-based aging factor for refreshing the value of **β** which is defined as follows: $\tau_q(t) = \mu \times \frac{\beta(t)}{\beta(t)+1}$ where μ is constant (set to 0.6). The value of $\mu > \gamma$ so as to punish misbehavior with an intensity greater than the reward 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**. As the variables **α** and **β** are updated periodically, the values of belief, disbelief and uncertainty are also updated accordingly. The values of p and q are initialized to zero after the update of $\alpha(t+1)$.

5. Proposed 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
- 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. The number of recommendations which are selected are fixed denoted by R. 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. Figure.1 below shows the working and the interdependency of each of the modules which collaboratively work to provide the functionality of the proposed RecommFilter scheme.

5.1 Recommendations Selection 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 denoted by . 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 following order of priority:

1. The nodes upon whom the subject node has a recommendation trust with a belief component greater than 0.5
2. i. The nodes upon whom the subject node has a direct forwarding trust with a belief component greater than 0.5
   ii. The nodes upon whom the subject node has a similarity index of value greater than 0.5
3. Remaining one-hop neighbors

The nodes within each of the first two categories are sorted in the descending order of their belief component of the corresponding trust / similarity index and further the sub-categories 2.i and 2.ii are placed at the same level of priority. From the sorted list of recommenders, the recommendations from the first R recommenders will be selected.

5.1.1 Computation of Similarity Index

Similarity index between two nodes refers to the extent of match in the opinions expressed in the form of direct trust upon their common neighbors. The similarity index between two nodes is computed with respect to opinions/trust formed about other peers regarding their packet forwarding behavior. It involves the usage of principled distance between two bodies of evidence as proposed in [20] referred to as Jousselmes distance.

The proposed security mechanism incorporates a trust framework wherein the indirect trust computation module utilizes the approach proposed in [21] which leverages on the collaborative filtering. The main idea is when a subject node has trust preferences on certain nodes similar to some target node then, the credibility of the target node as a recommender would be higher. Hence the recommender selection module finds out the similarity index between a subject node and its neighbors to decide which of them should be selected as recommenders.

The similarity index between two nodes i and k can be computed as follows:

$$S_{i,k} = \frac{\sum_{u \in CN_{i,k}} \left[1 - \Delta\left(T_{i,u}{}^{D},\ T_{k,u}{}^{D}\right)\right]}{\left|CN_{i,k}\right|}$$

Where $CN_{i,k}$ represents the common neighborhood of nodes i and k, $T_{i,u}{}^{D}$ represents the direct trust of node i upon node u and $T_{k,u}{}^{D}$ represents the direct trust of node k upon u

The motivation behind using the collaborative filtering based approach of using the similarity index to decide the credibility of the recommender is that the subject node i need not necessarily have direct trust with non-zero belief component upon all its neighbors. It might be possible that the subject node i had interacted with very few of its neighbors meaning that, it is completely uncertain about the forwarding characteristics of most of the neighbors. In such circumstances, node i would end up with very few recommenders or no recommenders at all. To cope up with such situations, there should be certain additional criteria to choose a recommender. Even though node i may not have a non-zero belief direct trust, node i and node k may have similar trust preferences upon their common neighbors which serves as the criteria for recommender selection.

5.2 Recommendations Filtering Module

The module aims to filter out certain recommendations from 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 proposed trust framework incorporates a recommender filtering module which utilizes an algorithm based upon clustering similar to approach proposed by Yu et al.[12] wherein the recommendations with least distance/dissimilarity or maximum similarity are merged into one cluster. The approach proceeds to generate a fixed number of clusters denoted by K (set to K=R/4). Initially, each recommendation individually is treated as a separate cluster and two clusters with maximum similarity are merged together into a single cluster. From the resulting set of clusters, the same action of finding two clusters with maximum similarity and merging them together is performed to generate a new set of clusters. The clusters generated in each step act as input to the next successive step and the process of identifying two clusters with maximum similarity and merging them into one is repeated until the specified number of clusters generate. From the K clusters that have been generated, the cluster with maximum number of recommendations is selected by applying the majority rule. Hence the two major actions which comprise the algorithm

are:

- Computation of Opinion Similarity Measure between two clusters
- Merging of two clusters by combining the recommendations

5.2.1 Computation of Opinion Similarity Measure between two clusters

The similarity between two clusters is represented by the opinion similarity measure. Opinion similarity measure involves the generation of distance between the opinions about a specific node k expressed in the form of direct trust by two different subject nodes i and k or in the form of an integrated trust by two different clusters.

When opinion similarity measure has to be computed between two nodes, it can be represented as $OS_{i,k}{}^{j} = 1 - \Delta(T_{i,j}{}^{D}, T_{k,j}{}^{D})$ where $OS_{i,k}{}^{j}$ represents the opinion similarity measure of subject nodes i, and k with respect the packet forwarding behavior of node j,

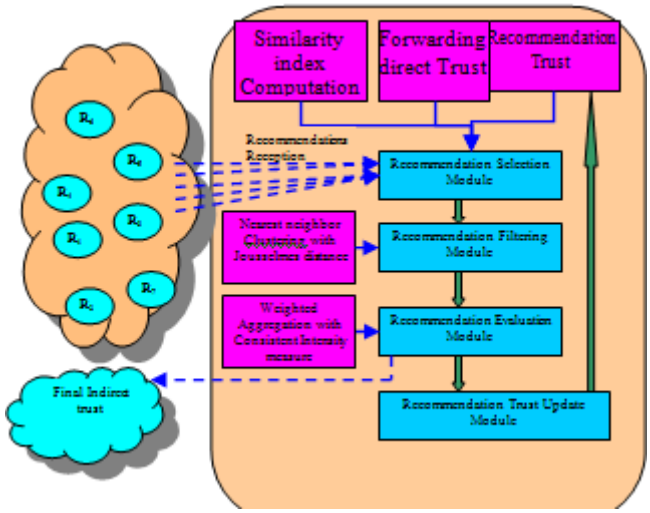

Figure 1: Overview of RecommFilter Scheme

$\Delta(m_1, m_2)$ represents the Jousselmes distance between two basic probability assignments (bpa) represented by m_1 and m_2 respectively. Specific to the proposed trust framework, since the trust of a subject node upon an object node j is represented through subjective logic using the Dempster Shafer theory in the form of a tuple (b, d, u) and the composition of trust comprises of basic probability assignment or body of evidence, Jousselmes distance represents a measure of opinion difference wherein $0 \le \Delta(m_1, m_2) \le 1$.

$$\Delta(m_1, m_2) = \sqrt{\frac{1}{2}\left(\|\vec{m}_1\|^2 + \|\vec{m}_2\|^2 - 2\langle \vec{m}_1, \vec{m}_2 \rangle\right)}$$

Where $\|\vec{m}_1\|^2 = \langle \vec{m}_1, \vec{m}_1 \rangle$ and $\|\vec{m}_2\|^2 = \langle \vec{m}_2, \vec{m}_2 \rangle$

$\langle \vec{m}_1, \vec{m}_2 \rangle$ is the scalar product of defined by

$$\langle \vec{m}_1, \vec{m}_2 \rangle = \sum_{i=1}^{2^\Omega} \sum_{j=1}^{2^\Omega} m_1(A_i) m_2(A_j) \frac{|A_i \cap A_j|}{|A_i \cup A_j|}$$

Where $A_i, A_j \in 2^\Omega$ for i, j = 1, 2, ..., 2^Ω and 2^Ω ={{T},{-T},{T,-T}}. Hence the value of $\Delta(m_1, m_2)$ can be computed using the values of $\|\vec{m}_1\|^2$, $\|\vec{m}_2\|^2$ and $\langle \vec{m}_1, \vec{m}_2 \rangle$ which have to be computed as depicted in the equations above.

If m_1 and m_2 represent the opinion of some node A upon the behavior of another node B and the opinion of some node C upon the behavior of node B, then the Jousselmes distance can be computed to obtain a quantitative measure of the difference of opinions of nodes A and C with regard to the behavior of node B. The opinion similarity measure is then computed as follows:

$$OS_{A,C}{}^{B} = 1 - \Delta(m_1, m_2)$$

According to literature, the distance between two clusters consisting of multiple data points is the distance between their centroids (which is computed as the mean of the data points within the cluster). In the proposed trust framework's recommendations filtering module, the clusters consist of recommendations represented in the form of basic probability assignments (bpa) or body of evidence. Hence the centroid of cluster implies the combined / integrated opinion of all the recommendations present within the cluster. It can be obtained through the Dempsters rule of combination or the orthogonal sum upon the bpas within the cluster. The process of generating the integrated opinion involving each of the recommendations within the cluster is performed when merging two clusters.

5.2.2 Merging of two clusters by combining the recommendations

The process of merging two clusters or more specifically two or more recommendations into one cluster implies that each cluster consists of one or more recommendations. The end result of the merging process is the integrated opinion computed using the D-S combination rule which represents the centroid of the cluster and also the individual recommendations which form the members of the cluster. The D-S combination rule is explained as follows:

Let $m_1(A)$ and $m_2(A)$ are the basic probability numbers or evidences which are in the same frame of discernment obtained from two independent observers. The Dempsters rule for combination consists of the orthogonal sum:

$$m(A) = m_1(A) \oplus m_2(A) = \frac{\sum_{i,j:A_i \cap A_j = A} m_1(A_i) m_2(A_j)}{\sum_{i,j:A_i \cap A_j \neq \phi} m_1(A_i) m_2(A_j)}$$

Similarly, if evidences are obtained from more than two observers, then the same combination rule can be extended:

$$m(A) = (((m_1(A) \oplus m_2(A)) \oplus m_3(A)) \oplus \cdots) \oplus m_s(A)$$

D-S combination can then be used to obtain the belief, disbelief and uncertainty components of the aggregated recommended trust through the integration of recommendations from the selected recommenders using the following formulae:

Let m_1 and m_2 represent two opinions which have to combine and let the basic probability assignment defined by m_1 and m_2 are represented as follows:

$m_1(\{T\}) = b_1$, $m_1(\{-T\}) = d_1$ and $m_1(\{T, -T\}) = u_1$

$m_2(\{T\}) = b_2, m_2(\{-T\}) = d_2$ and $m_2(\{T, -T\}) = u_2$
Then

$$m(\{T\}) = m_1(\{T\}) \oplus m_2(\{T\}) = \frac{1}{K}(b_1 b_2 + b_1 u_2 + b_2 u_1)$$

$$m(\{-T\}) = m_1(\{-T\}) \oplus m_2(\{-T\}) = \frac{1}{K}(d_1 d_2 + d_1 u_2 + d_2 u_1)$$

$$m(\{T,-T\}) = m_1(\{T,-T\}) \oplus m_2(\{T,-T\}) = \frac{1}{K} u_1 u_2$$

Where

$$K = b_1 b_2 + b_1 u_2 + b_2 u_1 + d_1 d_2 + d_1 u_2 + d_2 u_1 + u_1 u_2$$

Since $\{T\} = \{T\} \cap \{T\}, \{T\} = \{T\} \cap \{T,-T\}$, $\{-T\} = \{-T\} \cap \{-T\}, \{T,-T\} = \{T,-T\} \cap \{T,-T\}, \{T\} \cap \{-T\} = \phi$ and $\{-T\} \cap \{T\} = \phi$. The symbol $\oplus$ represents the D-S combination operation between different pieces of evidence also called as "direct sum" . The cluster which is generated as the output of Recommendations Filtering module is given as input to the Recommendations Aggregation module.

5.3 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 involves the functionality of recommendations aggregation to form a more refined final indirect trust value.
The evaluation module involves two stages. The first stage utilizes a consistent intensity based model using the opinion similarity measure among all the recommendations to generate a weight for each of the recommendations. The second stage combines the weighted recommendations using the Dempsters rule of combination to generate the final indirect trust.

5.3.1 Recommendation Aggregation using Consistent intensity Weights

The recommendation aggregation mechanism has to incorporate an adjustable and flexible model to minimize the impact of false recommendations through malicious nodes. Hence the proposed mechanism is based upon the approach proposed in [22] which adopts a consistent intensity to adjust weights of the recommended trust values. The motivation behind the usage of the said model for adjusting the weights of recommendations is as follows: Within the cluster provided as input by the recommendations filtering module, those recommendations which are relatively distant from the majority of the other recommendations have to be given lesser weight while computing the final indirect trust. The consistent intensity is nothing but the opinion similarity measure between two recommendations (say ${T_{a,k}}^D$ and ${T_{b,k}}^D$) which is defined is as follows:

$${I_{a,b}}^k = 1 - \Delta({T_{a,k}}^D, {T_{b,k}}^D)$$

Where ${T_{a,k}}^D$ represents the recommendation of node upon node k (which is nothing but its direct trust), ${T_{b,k}}^D$ represents the recommendation of node b upon node k and $\Delta({T_{a,k}}^D, {T_{b,k}}^D)$ represents the Jousselmes distance between ${T_{a,k}}^D$ and ${T_{b,k}}^D$ whose computation is described above.

As the value of consistent intensity reduces, the probability of false trust recommendations also decreases. The matrix of consistent intensity including all the recommended trust values is defined as follows. Here the nodes which provide recommendations are named as a, b, c, d, …..s.

$$\begin{bmatrix} 1 & {I_{a,b}}^k & \cdots & {I_{a,s}}^k \\ {I_{b,a}}^k & 1 & \cdots & {I_{b,s}}^k \\ \vdots & \vdots & \ddots & \vdots \\ {I_{s,a}}^k & {I_{s,b}}^k & \cdots & 1 \end{bmatrix}$$

The summation in row and normalization is performed to generate the total consistent intensity of the recommendation ${T_{a,k}}^D$ which is represented by ${I_a}^k$. It is defined as follows:

$${I_{i,k}}^a = \frac{\sum_{v=1, v \neq u}^{s} {I_{i,k}}^{u,v}}{Max\left(\sum_{\substack{v=1, v \neq w \\ 1 \leq w \leq s}}^{s} {I_{i,k}}^{w,v}\right)}$$

The total consistent intensity is generated for each recommended trust ${\vec{T}_{i,u-k}}^R$ for all u=a,b,c,….s. The recommended trust components of ${\vec{T}_{i,a-k}}^R$ represented as $\left({b_{i,a-k}}^R, {d_{i,a-k}}^R, {u_{i,a-k}}^R\right)$ are modified using the value of total consistent intensity ${I_{i,k}}^a$: ${b'_{i,a-k}}^R = {b_{i,a-k}}^R \times {I_{i,k}}^a$, ${d'_{i,a-k}}^R = {d_{i,a-k}}^R \times {I_{i,k}}^a$, ${u'_{i,a-k}}^R = {u_{i,a-k}}^R \times {I_{i,k}}^a$ The modified recommended trust from each of the selected recommenders is used to perform recommendation aggregation. The generation of the modified recommendation trust values is followed by their combination using the Dempster-Shafer combination rule which is explained in section 5.2.2.

5.4 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.

Assume that node X receives the indirect trust values from nodes A, B, C in the trust update period t-1. The computation of the indirect trust value for some node Y is done by the evaluating node X using the Recommendation Selection module, Recommendation Filtering module and Recommendation Evaluation module as described above. The evaluating node X compares its direct trust values for the other nodes as computed by its direct experiences in the current trust update period t with the corresponding indirect trust values as provided by the recommenders of the earlier trust update period and updates the recommendation trust of each of the recommenders. The comparison of the indirect trust value and the direct trust value is done using the

Jousselmes distance used to compute the distance between two bodies of evidence.

The recommendation trust is represented in the same way as the forwarding / direct trust leveraging upon the Dempster Shafer theory for the quantification of uncertainty (as described above). The mapping of the variables α and β to the tuple (b, d, u) and the update of α and β is the done in the same way as forwarding trust except that α indicates a positive recommendation event and β indicates a negative recommendation event.

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 (set to 0.05). If the deviation crosses the threshold, then a negative event is counted.

3. Performance Evaluation

The simulation experiments of the proposed scheme are carried out through network simulator 2 using the Trust-AODV routing protocol [23]. The trust model is based upon Dempster Shafer theory of evidence as explained above in section 4. The performance of the proposed scheme is compared with RecommVerifier(RV) [11], E-Hermes(EH) [4] (based on personal experience) and Whitby's filtering scheme(WFS) [6] (based on majority rule).

3.1 Simulation Methodology

In the simulation experiments, each network node may involve itself in two services: forwarding data packets and propagating/sending recommendation packets consisting of direct trust values of known nodes (nodes upon whom uncertainty is less than 1). A node may exhibit malicious behavior in either of the two services. As a data packet forwarder, it can either forward the data packets in case of non-malicious behavior or it can drop the data packets in case of malicious behavior. Similarly, as a recommendation provider, it can either provide honest recommendations or dishonest/false recommendations. 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 and 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. Three attack methods (i.e. slandering, self-promoting and collusion) are carried out and the effect of dishonest recommendation is examined. The performance of the proposed security scheme is analyzed with respect to a significant varying parameter which is the percentage of dishonest recommenders.

3.2 Metrics to analyze the impact of Dishonest Recommendations

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. To measure the efficiency of the Recommendation Trust Update (RTU) module and its role in the detection of dishonest recommenders, we consider two different scenarios wherein the first one has the RTU module disabled whereas the second one has the RTU module disabled.

Three different attacks of slandering, self-promoting and collusion are considered in the two scenarios described above (with RTU enabled and RTU disabled). The metrics used are the proportion of false positives and the false negatives (FPP and FNP respectively).

Table 1: Experimental Parameters

Parameter	*Value*
Coverage area	800m X 800m
Normal nodes	50
Speed	0 to 50 m/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	Random way point model
Traffic type	UDP – CBR (Constant Bit Rate)
Packet size	512 bytes
Pause time	1 s

m = meter, s = second

False Positives Proportion: The percentage of honest recommendations which are wrongly detected as dishonest ones.
False Negatives Proportion: 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 and Fig. 3 show the FPP and FNP with RTU enabled/disabled for the three attacks of slandering, self-promoting and collusion, 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% and RTU disabled, at the time instant 900 seconds the FPP and FNP is 74% and 78% respectively which is very much higher compared to FPP and FNP with RTU enabled which are 10% and 5% respectively. With the passage of time, the decrease in the FPP and FNP is also very less since the true nature of a dishonest recommender is not revealed as the RTU module is disabled.

In Fig. 2, it can also be observed that, the decrease in the FPP and FNP within a period of 800 seconds is 16% and 14% respectively with RTU disabled whereas the RTU enabled, it is 78% and 80% respectively. With RTU module enabled, the true nature of more and more dishonest recommenders is revealed with time and hence the FPP and FNP also decrease drastically with time.

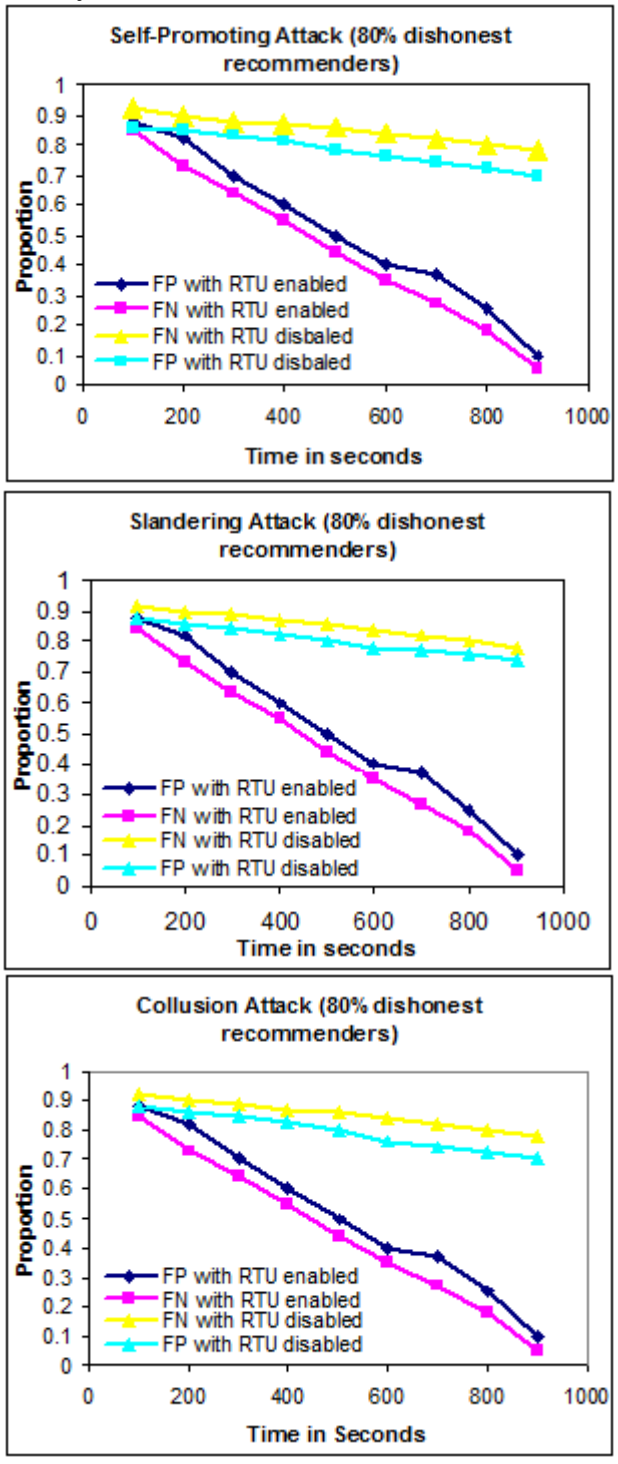

Figure 2: False Positive Proportion and False Negative Proportion for Slandering Attack, Self-Promoting Attack and Collusion Attack with 80% dishonest recommenders dishonest recommenders

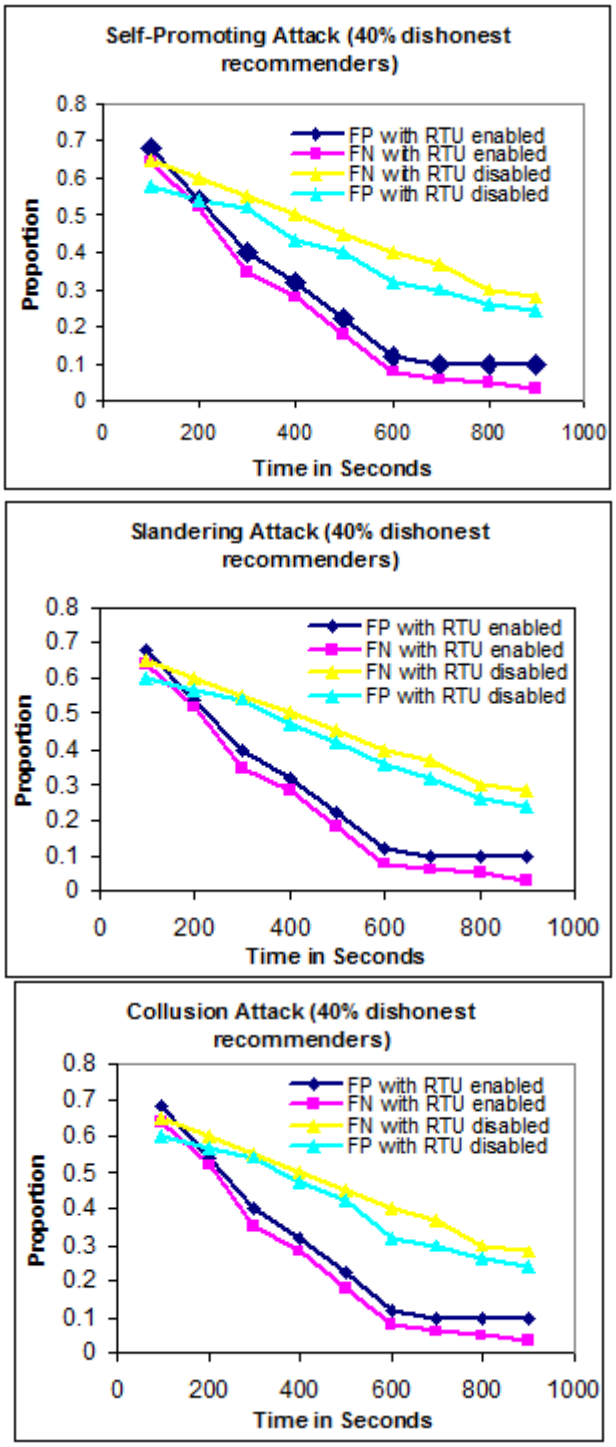

Figure 3: False Positive Proportion and False Negative Proportion for Slandering Attack, Self-Promoting Attack and Collusion Attack with 40% dishonest recommenders dishonest recommenders

Another important observation is that, even if the RTU is module disabled, the FPP and FNP do not remain constant in time but decrease by small amounts (16% and 14% respectively) as the precedence/priority rules in the recommendation selection module based upon the forwarding trust and the similarity index also contribute to a certain extent in the detection of true dishonest recommenders but the extent of contribution is quite small compared to the contribution of recommendation trust obtained through the RTU module.

The change in the FNP metric is the same for slandering attack, self-promoting attack as well as collusion attack for both the cases of RTU enabled as well as RTU disabled as can be observed in Fig.2 and Fig.3. The FPP metric with RTU disabled in the self-promoting attack has a decreased false positive rate compared to slandering attack and collusion attack, since the attackers now target upon manipulating the trust to be on the higher side unlike the slandering attack.

In Fig.3, it can be observed that when the percentage of dishonest recommenders is 40%, the FPP and FNP with all the three attacks are much lesser when compared to the FPP and FNP with 80% dishonest recommenders. Apart from the FPP and FNP, another metric used for performance analysis is the 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 three other schemes: the RecommVerifier Scheme [11] which overcomes lots of limitations of existing defense schemes using the majority rule based approach along with two other novel mechanisms of Time Verifying and Proof Verifying but the trust model is based upon Bayesian inference, the E-Hermes scheme [4] which is based upon the personal experience based approach and the Whitby's filtering scheme based upon majority rule based approach [6].

The trust convergence rate is studied in two scenarios: one with 40% dishonest recommenders and the other with 80% dishonest recommenders. Two different types of nodes with two different attack types are considered: One is a good/non-malicious node with slandering attack and the other is bad/malicious node with self-promoting attack. The slandering attack causes a good node's trust to reduce in the initial trust update period but with more number of trust updates, the deployment of a defense scheme causes the trust to improve gradually and at one point in time, the computed trust becomes almost equal to the actual trust reflecting its true nature. Fig. 4 and Fig. 5 show the trust convergence rate for two different scenarios : one with 80% dishonest recommenders and another with 40% dishonest recommenders for the two attacks, slandering attack and self-promoting attack. It can be observed that, in case of 80%

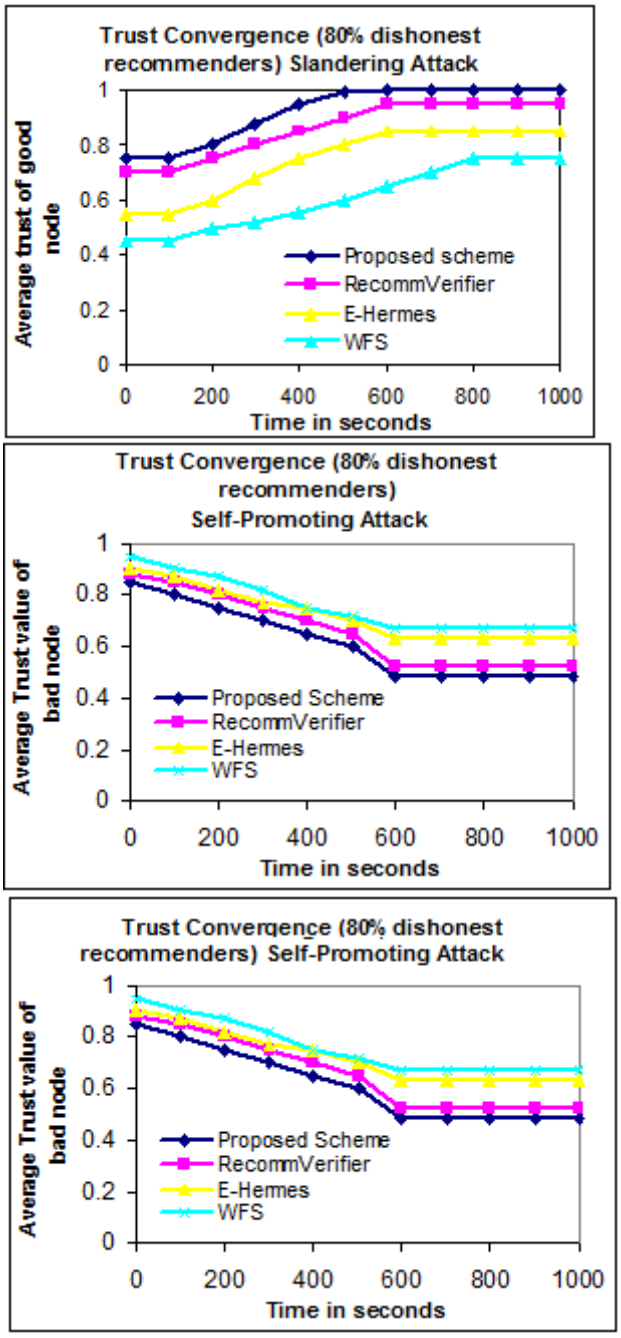

Figure 4: Trust Convergence rate of a good node and a bad node with Slandering and Self-Promoting attacks respectively with 80% dishonest recommenders

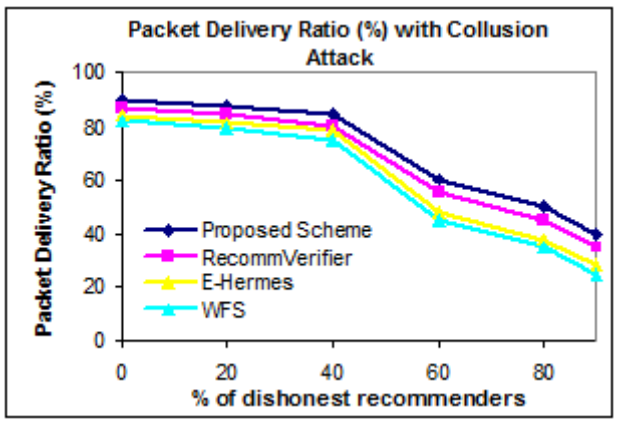

Figure 6: Packet Delivery Ratio

dishonest recommenders, the computed trust of a good node

as well as bad node converges at 600 seconds after which the computed trust remains constant with time. Fig. 4 and Fig. 5 show the comparative analysis wherein the proposed RecommFilter scheme outperforms all the remaining three schemes.

In case of slandering attack as well as self-promoting attack, the convergence of trust using the RecommFilter scheme is closest to the actual trust metric reflecting the true nature of the node. In the 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. The WFS scheme performs the least compared to all the other schemes as it is based only upon majority rule based approach which may obscure many dishonest recommenders and result in the slowest convergence rate.

With 40% dishonest recommenders, the trust convergence rate for slandering attack and self-promoting attack are shown in Fig. 5. It can be observed that as number of dishonest recommenders decreases, the trust convergence rate is faster at 400 seconds (compared to 600 seconds with 80% dishonest recommenders) since the true nature of a node is revealed faster.

The comparative analysis also shows that, the proposed RecommFilter scheme performs better compared to RecommVerifier, E-Hermes and WFS schemes irrespective of the number of dishonest recommenders by having the computed trust closest to the actual trust reflecting its true nature. Another metric used for comparative analysis is the packet delivery fraction by varying the number of dishonest recommenders.

Packet delivery fraction is computed as the ratio of total number of packets received by the destination to the total number of packets sent by the source node. As expected, for all the schemes, as the number of dishonest recommenders increases the packet delivery fraction decreases. Fig. 6 shows that the proposed RecommFilter scheme has the highest average packet delivery fraction of 68.83% compared to 64.5%, 59.5%, and 56.83% of RecommVerifier, E-Hermes and WFS. Since the packet delivery fraction is directly proportional to the efficiency of trust model (since trust based routing is employed) which includes the efficiency in detection of dishonest recommenders, it is obvious that the proposed RecommFilter outperforms the remaining three schemes.

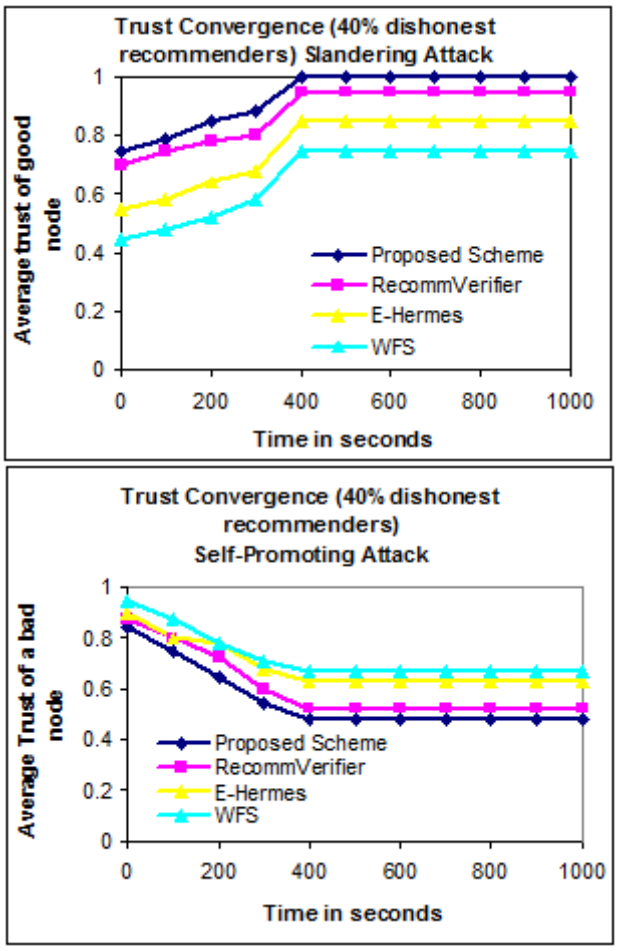

Figure 5: Trust Convergence rate of a good node and a bad node with Slandering and Self-Promoting attacks respectively with 40% dishonest recommenders

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 modules of Recommendation Selection, Recommendation Filtering, Recommendation Evaluation and Recommendation Trust Update work together collectively to efficiently detect dishonest recommenders with a reduced false positive proportion and a reduced false negative proportion. The recommendation selection module ensures that irrespective of the number of recommendations received, the precedence rules enable the selection of a fixed number of recommendations. The recommendation filtering module accepts as input the recommendation set obtained as the output of recommendation selection module. The input recommendation set is used to select a subset which represents a refined recommendations set. The

recommendation trust update module assists the recommendation selection module in choosing a subset of relatively credible recommendations out of the received set of recommendations. The simulations experiments show that the proposed RecommFilter scheme works efficiently even in the presence of 80% dishonest recommenders.

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] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc.IEEE, vol. 98, no. 10, pp. 1752–1754, Oct. 2010
[3] M. Carbone, M. Nielsen and V. Sassone, "A formal model for trust in dynamic networks," in In Proc. International conference on software engineering and formal methods, SEFM03, pp. 54–63, 2003
[4] 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.
[5] S. Ganeriwal, L.K. Balzano, M.B. Srivastava, Reputation-based framework for high integrity sensor networks, ACM Transactions on Sensor Networks 4 (2008) 1–37
[6] 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.
[7] J. Feng, Y. Zhang, H. Wang, A trust management model based on evaluation in p2p networks, IEICE Transactions on Information and Systems 93 (2010) 466–472.
[8] 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.
[9] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Transactions on Knowledge and Data Engineering 16 (2004) 843–857.
[10] R. Zhou, K. Hwang, Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing, IEEE Transactions on Parallel and Distributed Systems (2007) 460–473
[11] 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
[12] 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
[13] S.Buchegger, and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems, " Communications Magazine, IEEE, pp. 101-107, 2005
[14] 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
[15] N. Wilson, "Algorithms for Dempster-shafer theory," in Algorithms for Uncertainty and Defeasible Reasoning, pp. 421–475, Kluwer Academic Publishers, 2000
[16] A. Josang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, 2002, pp. 324–337.
[17] F. Li, J. Wu, Mobility reduces uncertainty in MANETs, in: Proceedings of INFOCOM'07, 2007, pp. 1946–1954
[18] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, 1976
[19] A. Josang, Trust-based decision making for electronic transactions, in: Proceedings of NORDSEC'99, Stockholm University, Sweden, 1999
[20] 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
[21] J.L. Herlocker, J.A. Konstan, L.G. Terveen and J.T. Riedl, "Evaluating collaborative filtering recommender systems", ACM Trans. Information Systems, Vol.22, no.1, pp.5-53, 2004
[22] R. Feng, S. Che, X. Wang, and N. Yu, "A credible routing based on a novel trust mechanism in ad hoc networks," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 652051, 12 pages, 2013
[23] X. Li, M. R. Lyu, and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," in Proc. Aerospace Conference, IEEE, Vol. 2, pp. 1286-1295, 2004

Author Profile

Shirina Samreen did B.Tech in Computer Science & Engg from JNTU, Hyderabad, A.P., India in 2003 and M.Tech in Computer Science from JNTU, Hyderabad, A.P., India in 2006. She is currently working towards the Ph.D degree in the Department of Computer Science & Engineering, Jawaharlal Nehru Technological University, Hyderabad, A.P., India. She worked at various Engineering colleges and has 10 years technical teaching experience. Her current research interests include wireless security, secure routing, and trust management frameworks.