International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Trust Computation using Belief Model in Mobile Ad Hoc Network Avoiding Ballot Stuffing and Bad Mouthing

Hiteishi Diwanji

Abstract: ***Trusted path in MANET ensures packet delivery and reduces the packet dropping which results in a saving of bandwidth and energy of the mobile node. Trust path finding mechanism has been proposed in the literature based on direct and indirect observations and applying Bayesian theory, Dempster-Shafer theory involving probability logic. In this paper, we studied trust computation problem in MANET with predefined fixed movement and random movement (frMANET) to compute trust to get over bad mouthing and ballot stuffing. Our scheme(frMANET scheme) is based on subjective logic based belief model involving uncertainty in behavior. We use consensus for parallel paths and discounting for transitive paths. We use public key based digital signature to deal with nonrepudiation. This identifies the node if denying that it is bad mouthing or ballot stuffing. Unlike trust management in a conventional scheme that computes trust based on packet dropping and forwarding, we have added a parameter - state of the node indicating priority work and unable to participate notification. We include service rating as well considering file sharing and file downloading as service rating parameter. We have evaluated University case study of a course offered by a professor in university to the enrolled and not enrolled students. The simulation results show an increase in packet delivery ratio with marginal overhead in average message transmission. The scheme helps in avoiding unnecessary fluctuations in trust values of trustworthy nodes and also ensures less computational overhead. This research is helpful when communication is frequent and failure of delivery of message is not tolerable in MANET and nodes need to be rated for goodness.***

Keywords : MANET, logic, belief model, Security, trust and reputation management.

I. INTRODUCTION

Forming a mobile ad hoc network of nodes for routing and data sharing has been useful as minimum efforts are needed to set up the network. Trust is crucial as it helps in decision making to the nodes, such as which nodes to rely on for routing the packets as well as getting the services such as file download and file sharing. The node which is dropping the packets, delaying the packet forwarding, not allowing downloads of the file or not sharing the file are considered malicious and their trust decreases with each such behavior. The most trustworthy node can also exhibit such behavior in case it is doing some priority work.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Hiteishi Diwanji*, Information Technology department, L.D.College of Engineering, Ahmedabad, India. Email: Hiteishi@ldce.ac.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

In that situation, trust computation engine, decreases the trust and most trustworthy node is categorized as a malicious node. In that case, communication will be done through less trustworthy nodes. In the worst case, no communication path can be found having trust greater than threshold value. We have considered node state while computing trust, in case of high priority state, no decrease in trust values is observed. Trust computation schemes are often the victim of false praise and false criticism leading to wrong trust value ending up in untrustworthy paths.

In MANET, there is no central authority to monitor. Highly dynamic nature of the network, does not allow pre computed fixed secure routes to be used to forward packets from one node to another. A node may need other nodes to route packets. This type of open network can not be bound by any security policy defined by the owner of the information. Cryptographic security mechanisms for providing confidentiality of communication and authentication of nodes will not help against packet dropping and delayed packet attack or rushing attack nor it can help in rating the services.

In this paper we have defined the scheme based on subjective logic based belief model to establish trusted path for routing in ad hoc network protecting against bad mouthing and ballot stuffing and achieve an increase in throughput in mobile ad hoc network considering fixed and random movement. We also include state of the node while updating trust value. In the case of higher priority work, if the node does not participate in communication, it is not considered as malicious behavior. Our approach is based on the well proven mathematical model.

This paper is arranged as follow: in Section II presents the related work. In Section III we discuss the proposed approach. Simulation results are shown in section IV. We conclude this paper in Section V.

II. RELATED WORK

All approaches uptil now followed probabilistic logic with a binary opinion. They consider packet dropping or forwarding. The additional parameters in computation are file download is permitted. Every time uncertainty is involved in the behavior. We have used subjective logic based belief model for conditional reasoning. Our aim is to consider mobility model and state of the node in computing trust. The biased opinions must be neutralized. We use digital signature so that node cannot deny the fact that it provided biased opinion.

Mobility includes moving on the fixed path during the cycle and moving in a random direction. State of the node includes prioritized state, in which it cannot participate in routing and packet forwarding. This behavior in priority state not considered as misbehavior.

We have considered the movement and communication pattern of college students as well as the professor who is conducting the course. College students and professor has fixed classroom and tutorial schedules. College students have some non-predefined movement as they participate in extra activities. Professor and students may be involved in priority task, in that case, they neither participate in routing and packet forwarding nor provide services without any bad intention.

The model has five components to evaluate trust

(a) The individual opinion is subjective so we use stochastic Markov model and use belief model based on subjective logic. Uncertainty is inherent in the behavior of the node.

(b) We have used fixed (defined) mobility and random walk mobility, we call it frMANET.

(c) The nodes of MANET have the priority set. If it is doing some priority work, it may not participate in packet forwarding. In that case, trust value is not updated. The trust aggregation is based on subjective logic operators consensus and discounting to neutralize the bad mouthing and ballot stuffing attack.

(d) The nodes, who have registered in the MANET, may form subgroups among them. They move around in clusters. Within the subgroup, only one node communicates with one node in another group so fewer chances of interference. When there is inter- cluster or intra-cluster communication, the MAC mechanisms handle the node interference.

(e) Public key based digital signature ensures that the node giving biased opinions cannot deny the fact that it did not send the biased opinion.

We have considered packet forwarding and packet dropping, file sharing, file downloading as the parameter for calculating trust. Our contributions in this paper are: 1) we consider the fixed and random movement and finding the nodes which can be blacklisted. 2) We use stochastic Markov model which reduces the storage overhead of keeping history of behavior. 3) To neutralize the biased opinion, we use consensus and discounting operator. 4) To avoid zigzag between nodes being trustworthy to node being blacklist, we keep node state assuming that in priority state node is neither participating in routing nor in service providing. We evaluate the performance in terms of effect on throughput, complexity and resource consumption in computing trust.

The assumption we have made is the node participating in routing and information exchange are authentic nodes. The scheme uses public key cryptography to deal with nonrepudiation.

A. *Trust And Reputation Based On Bayesian Theory*

In [2] Buchegger S. et el. suggested a robust theory for calculating trust and reputation based on Bayesian theory. Reputation rating denoted by Ri,j is defined by two numbers(α', β'). It is updated on 2 types of events (1) when first-hand observation is updated (2) when a reputation rating published by some other node is copied. In this the scheme is robust. The nodes monitor the behavior of neighboring nodes by being in promiscuous mode, which consumes energy which is not desirable in wireless nodes. How much weight should be given to the past observation, how many past observations should be considered – these are the questions in this scheme. Maintaining multiple paths with ratings and choosing and avoiding paths based on ratings makes scheme complex and initial route set up taking time. If nodes are mobile and need to find routes frequently, then this scheme is costly in terms of route establishment. Once weight 0 is assigned meaning that node is not considering the second-hand information but later on a node needs the second-hand information, then how to increase weight to consider second- hand information is not mentioned.

B. *Trust Graph Based On The States And Locations Of Nodes At Time Points*

In [3] Zhao H. et el. gave theory to derive trust graph based on the states and locations of nodes at certain time. All the moving nodes are represented as a collection of states {X1,X2,..,Xn} which are vertices in trust graph. One node may have multiple states according to locations and time. In [3] to draw trust graph, locations of nodes are maintained. How to maintain locations and which node will maintain the position and the basis for establishing connectivity to draw graph is not clear.

The scheme considers all previous states. Constructing and maintaining this type of data structure and storing data in this form for mobile nodes is difficult. It even gets worst when large numbers of nodes are involved. If the node for some reason leaves the cyclic route the system reaction is not mentioned in the scheme.

C. *Computing The Service Quality*

In [4] Ayday E. et el. describes the way to compute the service quality (reputation) of the peers. Feedbacks are collected from the peers who used the service. The trustworthiness of the raters is determined by analyzing their feedback about service providers. Two types of system (i) The set of SPs(Service Providers) (ii) the set of Service Consumers are considered.

The global reputation of the jth SP and the rating that the rater i reports about the SP_j as TR_j and $Tr_{ij}.R_i$ denote the rating trustworthiness of the ith rater. In [4] generating and storing bipartite graph for a large number of nodes is difficult. Initially to generate the Bipartite graph, all raters and service providers information is to be gathered. The raters may have used different criteria to rate the service providers, which is not considered in the paper. The measurement of distance and the effect of mobility is not clear.

D. *Decentralized Object Reputation And Ranking System*

In [5] Walsh K. et el described Credence, a decentralized object reputation and ranking system for large-scale peer-to-peer file sharing networks. Credence depends on other peers to mark authenticity of the online content. When there is no way to determine trust on peers,

then peers often receive service from untrustworthy peers result in peers wasting resources on mislabeled content or may end up downloading Trojans.

In [5] Computation of trust and reputation is not mentioned. The scheme works well with a wired system having a client-server architecture. Calculations are done manually. Credence works for opinions on fixed attribute. The scheme involves too much manual work.

A. *Robust Trust and Reputation System*

In [13] Josang A. et el suggested how to measure strength of Trust and Reputation system(TRS). Authors emphasized that there are two main factors that affect the robustness. 1) TRS robustness 2) efforts by attackers. The strength of efforts by attackers can be modeled as increasing function of perceived incentives for attacking the TRS.

In our paper, we propose a trust model for information sharing in MANET environment assuming a university where professor and students interact to download and share data as well as help in packet forwarding. Nodes that are authentic can join and leave. Authentication is not part of our scheme. All nodes (students) who register for the course are pretrusted(fully trusted) initially. The course allows other students (students of other courses) to attend this course for the sake of knowledge gain. They are not pretrusted. Their trust value needs to be computed and they are denoted as new node(NN). We have used a state called high priority where a professor and student are involved in an important work and no networking activity takes place, hence no state transition.

Considering existing literature which mainly uses probabilistic logic does not include uncertainty in the behavior of the good node. Our approach is different which considers fixed and random movement and also a state of the node before evaluating trust. This avoids unnecessary updating of trust of a good node in case of node behaving as malicious in the case of priority work. This paper presents realistic application scenario.

The use of the trust value is to be mapped with the access control policy to determine the access privileges given to nodes that are not registered prior to network setup or called as a new node (NN). Taking college activity of professors and students as an example, there are possibilities that to allow NN to get an access to data/information shared by the structured group, the initial trust of NN need to be determined. We assume that the node entering the network is authentic.

III. PROPOSED APPROACH

The main goal of trust computation in Mobile Ad-hoc Network is to establish trusted connection amongst each other. Trust plays an important role in Mobile ad hoc networks since the trust path computation can be done by considering ethical behavior and integrity of its members in delivering the packet to the destination, sharing and allowing downloads of files. This can be implemented by collaborative mechanisms such as trust and reputation system. Collaboration is productive only if all participants operate in an honest manner. When some nodes decide against cooperating with one another, they are called selfish node. The threats such as packet dropping, delayed packet or rushing attack are from nodes within the network- nodes behaving in such manner are called misbehaving nodes. The trust and reputation based scheme would give selfish nodes the incentive to cooperate and in the worst case, isolate the misbehaving nodes.

Trust can be gathered from direct experience and / or with the recommendation from other nodes.

In the case of college/university a professor and a student node or student(node) to student(node) communicate. In some cases, direct experience may not be available. We did experiment with a case study of professor, enrolled students and not enrolled students. These entities form ad hoc network for transferring notes, assignments, important messages, and submission of files, sharing and downloading files. For every transaction the node will update its local trust table using the discounting operator. Functional trust is the value of trust from whom(forwarder) the packet is received. Referral trust is the trust from sender to the forwarder. At the regular interval of 2 hours global trust computed for all nodes by taking randomly two peers and use consensus to find fused opinion. That would be done by a master of the group.

Subjective logic is a kind of probabilistic logic that explicitly takes uncertainty and belief ownership into account. Subjective logic is suitable for demonstrating and examining solutions involving uncertainty and incomplete knowledge. In mathematics w=b+d+u=1, b,d,u ϵ[0,1] where b,d,u represents belief,disbelief and uncertainty respectively.

TABLE I. Notations

Notation	Definition
TR_B^A	Trust of A on B built during routing
TS_B^A	Trust of A on B during when A has asked for some service from B.
TL_B^A	Local trust calculation
TG_B^A	Global trust calculation
w	Weight of the trust value based on the priority level assigned to nodes
ρ	Adjustment factor in case b+d+u>1
λ	Longitivity factor.

A. *Attacks Considered For Trust Systems*

While communicating in MANET following attacks affect the communication and design of trust and reputation based scheme.

1. Rushing attack – In reactive routing protocol, a node that needs a path to destination floods the route request packets in the network. Every node only forwards the first route discovery packet that it receives and drops the rest. The attacker rushes the route request packets.

2. Ballot stuffing attack – Malicious nodes praise the nodes having poor performance in terms of packet forwarding, packet delaying.

3. Bad mouthing attack – Malicious nodes give a negative opinion for the good nodes and increase disbelief. As a result good node is blocked.

4. Decoy attack - A decoy hides what an individual or a group might be looking for while providing service.

5. Nonrepudiation attack – The node always providing negative or positive opinion denies the fact that it is sending the negative opinion.

B. Security Evaluation of frMANET

In our scheme, the nodes pass belief, disbelief and uncertainty values in decimal ranging between 0 to 1. Reliable rater generates rating as per performance. The adversaries(ballot stuffing and bad mouthing) follow cumulative frequency distribution. The malicious raters follow human characteristics while criticizing or praising. Human beings either praise highly or criticize highly. This results in either high opinion or very low opinion. Analogy with human behavior, the sweet tongues praises extremely and sour tongues criticizes heavily. We have designed the scheme assuming that in small network 10% malicious raters and as network grows, it goes upto 30%. Analytically frMANET scheme outperforms Averaging and Bayesian approach. The computational complexity of frMANET is linear with number of nodes. frMANET is scalable and suitable for large scale systems.

C. Proposed Trust Model

Bayesian reputation system with binomial reputation score is used in the literature. In such cases probability is defined as positive or negative opinion. MANET always has uncertainty involved in terms of behavior because of movement or selfish behavior of nodes in MANET. We evaluated Trust and reputation computation engines - Summation or average, Hidden Markov, Bayesian Discrete models, Belief models, Fuzzy models, Flow models specified in [13]. Summation or average method is not efficient as it does not protect against ballot stuffing or bad mouthing attack. Hidden Markov model does not prove efficient as MANET involves parameters that cannot be prespecified because of the dynamic nature of MANET. Discrete models, flow models, fuzzy models do not provide relevant mathematical background for trust calculation in MANET.

We consider one cycle to be of one day of working hours(8 hours) from 10.00am to 6.00pm. Local tables maintained at nodes which are updated after every transaction. Global table is updated at GCs (Global Cycle Time) as per activity scenario. The nodes having trust values less than predefined threshold are blacklisted. At the end of cycles TIs (Total Iteration Cycle), the blacklisted nodes are allowed to participate, if the behavior observed is same, they are permanently blacklisted.

We have used belief models based on subjective logic.We have considered belief model, with beta distribution. Binomial opinion with (uncertainty) u>0, its equivalent probability representation is Beta pdf

$$E(Beta(p|\alpha,\beta)) = \alpha/(\alpha+\beta)=(r+Wa)/(r+s+W)$$

Where r is a number of positive opinions, s number of negative opinions and W is noninformative prior weight usually taken as 2.

$$\alpha=r+2a\ ,\ \beta=s+2(1-a)$$

The layout of the building is considered which contains classrooms, staff cabins and laboratory and other areas of the college where student-professor movements are observed. In frMANET, movement of professor node and student nodes is a combination of fixed and random movement.

D. Trust Graph

frMANET has fixed and random movement. The unit time is set to 60 minutes. Each node i moving has motion period time FRi. From the trace, consider nineteen nodes. The maximum motion time for subset of 3 nodes are FR1=120,FR2=180,FR3=240. The system motion cycle is FRs multiple of 60 and greater than the all node motion period time. FRs=60*GCD(FR1/10,FR2/10,FR3/10).

To represent the frMANET trust relationships, trust relationships are considered on undirectional graph. In a trust graph, based on states S:{X1,X2,..Xn}, the nodes are represented as vertices of the graph. One node can possess only one state at a time. The state is represented as i[Ti] where i is the node id and Ti is the time at which we have considered the state. Ti=60*n where n=1,2,3,4,5,6. The state for node 1 is represented as 1[T60*n].

Trust rating is a real number [0,1].In the graph undirectional link with trust rating is denoted by FRTV.

Definition 3.1(FRTV) : The FRTV is a vector of rating of trust regardless of direction and is a real number R in [0,1]. There is an edge from node i to node j if and only if Ri,j>0. The nodes are isolated if Ri,j=0 indicates i never put trust on j. Ri,j=1 indicates full trust. The trust rating is a performance measure of the node indicating how it performed on packet forwarding, service providing on each transaction. There is no negative rating. The self trust means trust of node on itself which is not considered. In our research, we calculate new trust based on immediate previous trust.

E. Trust Path Computation Problem

In frMANET, each node maintains local trust table. In the trust table, each row indicates the node id and trust rating for each node reachable or not reachable, based on global trust announcement. The whole idea is to communicate through precomputed trust rating. Assuming node i wants to communicate with node z having no interaction in past, it can communicate based on global trust announcement.

Definition 3.1(frMTP):In frMANET Maximum Trust Path is the path from node i to node z having the highest total of trust among the edges from i to z.

Definition 3.2(frTransferTrust) : In case node A has trust rating for B(bR_B^A , dR_B^A , uR_B^A , aR_B^A) and node B has a trust rating for C(bR_C^B , dR_C^B , uR_C^B , aR_C^B) then from node A to C,

trust is computed as (bR_B^A , dR_B^A , uR_B^A , aR_B^A) $\otimes$ (bR_C^B , dR_C^B , uR_C^B , aR_C^B)

Definition 3.4(frCombineTrust) : In case node A has trust rating for C(bR_C^A , dR_C^A , uR_C^A , aR_C^A) and node B has a trust rating for C(bR_C^B , dR_C^B , uR_C^B , aR_C^B) then from node A to C, trust is computed as (bR_C^A , dR_C^A , uR_C^A , aR_C^A) $\oplus$ (bR_C^B , dR_C^B , uR_C^B , aR_C^B)

F. frTrust Model

frTrust Model is discrete time stochastic model based on a set of states. Every state associates several action(for example ,to blacklist the node) to choose. The trust path finding process denotes x as current state, x' as next state. We model frMTP problem as combination of frTransferTrust and frCombineTrust. The state transition is Px,x'. For a node the possible states S:{X1,X2..Xn} are S:{high priority, forwarding, dropping, rushing}

P(xt+1=Xt+1|xt=X,) if Xt+1 $\notin$ {high priority}

The aim is to have a path with maximum trust rating. Discounting is applied when we consider indirect path.

$W\lambda Tx1,x2 \otimes W\lambda Tx2,x3 \otimes .... \otimes W\lambda Txt,xt+1$

λ is a discounting rate that considers lifetime of route and node neighborhood. For invalid lifetime, the λ is updated exponentially to have significant change in trust value of node. $0 \leq \lambda \leq 1$. $\lambda \varepsilon \{1, e^{-x}, e^{x}\}$

W is weight. W is considered to be the significance of opinion. We have categorized our nodes into high, medium and low categories as we have three categories of node.

$W \varepsilon \{high, medium, low\}$.

Trust value $TG_c < 0.5$, then node is blacklisted and not allowed to communicate. For deciding trust value of a new node, opinions are combined to generate opinion. Consensus is taken between two opinions of different nodes while deciding whether to trust new node.

Value updation is done based on updating the trust values of nodes involved in communication. For the malicious behavior linear decrement is performed so that the punishment is not harsh and node is not immediately black listed. We applied randomness in choosing the nodes whose opinions are combined to generate a global trust value. In case, a node does ballot stuffing and bad mouthing, its opinion is fused with opinion of the other node by applying consensus or discounting. The bad opinion is not nullified but its effect is diluted because of consensus operator.

$\min(T_B^A, T_C^B) \leq (T_B^A \otimes T_C^B) \leq 1$

G. Nonrepudiation

Node can keep on sending negative opinions or positive opinions leading to bad mouthing and ballot stuffing. We use RSA based digital signature to deal with nonrepudiation. We use 16 bit key so that computation is not heavy on node. The 16 bit key can be compromised by brute force attack. To avoid brute force attack, we frequently change public key-private key. This key computation can be done offline; hence communication overhead is not increased. We evaluated Elliptic Curve Cryptography for use. It is complex in use for MANET because of mobility and also loads a node with heavy computation.

H. Algorithm

The proposed scheme aims at calculating trust and reputation of a new node willing to enter the cluster and updating the trust value at regular interval. For this first-hand information about the node and second-hand information about forwarded and dropped packet by neighboring nodes, file sharing and file downloading services provided by neighboring nodes is taken into account. The purpose of the trust value is to determine that whether the node can be used for communication.

Case 1: calculate trust values for new node entering the group.

1) The Master of the group(MG) is the professor who conducts the course.
2) Let M be the members of the cluster and NN be new node willing to join the cluster.

$TR^{NN}=\{bR^{NN}, dR^{NN}, uR^{NN}\}=\{0,0,1\}$

3) NN enters the network and broadcasts a message to all nodes in the network. MG replies to NN in unicast mode.

TABLE II. Table Trust value and object sensitivity level

Trust value	Trustworthiness of Node
0<=TV <0.5	Not Trustworthy
0.5 >= TV< 1.0	Trustworthy

4) MG sends a packet to a new node with a timestamp. The new node will send back the same packet to MG and will also forward to neighboring nodes (P1 and P2) as part of handshake process.
5) Applying subjective logic to the proposed trust model

For successful packet delivery from NN to neighbor node P_1 update:

$$TR_{NN}^{P1}=\{bR_{NN}^{P1}, dR_{NN}^{P1}, dR_{NN}^{P1}\}=\{0.7,0,0.3\}$$

For unsuccessful packet delivery update:

$$TR_{NN}^{P1}=\{bR_{NN}^{P1}, dR_{NN}^{P1}, dR_{NN}^{P1}\}=\{0,0.7,0.3\}$$

The same way opinion of P_2 is considered.

6) Get the opinion of MG, call it T_1. Get the opinion of P_1 and P_2 for NN, get average and call it T_2. These two opinions are combined to get the consensus opinion[15].

7) Trust Value calculation, TV=0.4 T_1+0.6 T_2

Case 2: Updating the trust values of members of group at regular interval

1) Start Time quantum

2) When a packet is delivered to the destination(C), destination determines the node (B) who forwarded the packet and puts functional trust.

In the route table entry, the node(A) who forwarded the packet to B checks its trust value for B, which is said to be the referral trust.

To compute transitive trust, Discounting is used[12]. It is denoted by

$$TR_c^{A.B} = \{ TR_B^A \otimes TR_c^B \}$$
$$TS_c^{A.B} = \{ TS_B^A \otimes TS_c^B \}$$

3) Stop time quantum. To establish the trust value of C, Check the opinions of its 2 neighbors A and B respectively. To fuse two beliefs may be conflicting, the consensus operator is used.[12].

4) Calculate the weighted sum to compute trust. W is the weight assigned to each opinion depending on the node being professor(wp) or enrolled student student(wss) or not enrolled student (wjs).

$$TG_C = \alpha((w_1.TL_C^A \oplus w_2.TL_C^B)/2)$$

w1,,w2 ε {wp>wss>wjs} wp>wss>wjs

where α adjusting factor so that b,d,u in [0,1] and sum up to 1.

5) For packet dropping, delayed packet or early delivery - the belief, disbelief, and uncertainty is manipulated as follows. Linear decrement is chosen over exponential decrement as exponential decrement puts heavy punishment on node that would lead to hopping of node from trustworthy to untrustworthy and vice versa with a much larger difference. A node may unintentionally do dropping, delaying or early delivery. If x represents the set of state and x $\notin$ {high priority}

b= b- η_d (b>=0.01) otherwise b=0

d=d+ η_{id} (d<=0.99) otherwise d=1

u=u

For successful packet delivery

b= b+ η_{ib} (b<=0.98) otherwise b=1

d=d- η_d (d>=0.01) otherwise d=0

u=u- η_d (u>=0.01) otherwise u=0

6) If node is not participating in communication, aging factor is used to manipulate belief, disbelief and uncertainty by observing the markov model.

$$b_{new} = \lambda b_{old} \quad (43)$$
$$d_{new} = \lambda d_{old} \quad (44)$$
$$u_{new} = \lambda u_{old} \quad (45)$$

The random variables on which state transition depends are mobility of the node under consideration and lifetime of route that contains node under consideration. The node is within neighborhood, route lifetime is valid in routing table then λ = 1.

The node is not within neighborhood, route lifetime is valid.

λ = e $^{-x}$ for belief or λ = e ^{x} for uncertainty.

The node is within neighborhood, lifetime is not valid. λ = e $^{-x}$ for belief or λ = e ^{x} for uncertainty

There are 3 possibilities and each has equal probability. So x=0.33.

IV. SIMULATION RESULT

Procedure : We evaluate how reputation ratings develop over time by comparing honest and malicious nodes. Trust is computed in a decentralized manner, neither a professor node nor a single student node is taking responsibility of keeping trust score of all nodes. Each node establishes its own trust score while communicating. After a period of GCs (Global Cycle Time), professor node is computing the final trust score of each node applying consensus and discounting.

Security Evaluation and Adversary Models

A. *Ballot stuffing and bad mouthing*

Success of our scheme depends on how effectively the effect of bad mouthing and ballot stuffing is neutralized. The contact duration of two nodes is purely random and the number of times the information exchange occurs is also random. We have devised a scheme so that the probability of false positive and false negative is low. In our scheme it does not matter how much information has been transferred. Adversary nodes resembles human characteristic as humans either have characteristic of praising or criticizing or remain neutral giving honest opinion. Our adversary nodes either do ballot stuffing or bad mouthing as they are characterized as per human characteristics. To set threshold for ballot stuffing opinion or bad mouthing we did extensive study of behaviour of population of approximately 4000 nodes in our campus.

TABLE III. Trust value and object sensitivity level

Department	Samplesize	Belief rating range(higher)	Belief rating range(lower)	% node(bad mouthing)	% node(ballot stuffing)	% node(honest)
Rubber	76	0.85-0.95	0.65-0.75	10	50	40
IC	156	0.85-0.95	0.1-0.2	35	10	55

IT	359	0.85-0.95	0.45-0.65	5	45	50
Computer	363	0.85-0.95	0.25-0.35	15	30	55
Textile	134	0.85-0.95	0.25-0.35	5	50	45
Mechanical	374	0.85-0.95	0.1-0.15	35	10	55
Electrical	365	0.85-0.95	0.2-0.25	15	30	55
Environmen t	123	0.85-0.95	0-0	0	10	90
Automobile	114	0.85-0.95	0.1-0.2	10	10	80
Civil	374	0.85-0.95	0.1-0.15	45	10	45
Chemical	142	0.85-0.95	0.05-0.15	5	50	45
General	960	0.95-0.9	0.55-0.45	5	75	20
EC	274	0.85-0.95	0-0	0	25	75

We observed from sample studies that in case of ballot stuffing the node gives opinion value of belief between 0.8 to 0.95. The study reveals that for bad mouthing belief values range between 0.1 to 0.35. so we set the threshold for ballot stuffing 0.9 belief value. We set 0.2 belief value as threshold for bad mouthing. Our model follows Cumulative Distribution Function. According to function, belief value is 0.9 for ballot stuffing and 0.2 for badmouthing . If for every node a particular node is replying with 0.9 or above belief value than the node is ballot stuffing node. If for every node a particular node is replying with 0.2 belief value than the node is bad mouthing. The limit of 0.9 and 0.2 resembles the human nature of the behavior of extremely praising or criticizing. Human tendency is to praise or criticize, they do not mix praising and criticizing. Any opinion value between 0.2 and 0.9 is considered as honest opinion. We use Kolmogorov-Smirnov test to decide whether a node is ballot stuffing or bad mouthing by evaluating a particular node belief table to check whether all values are above or equal to 0.9 or all values are below or equal to 0.2. Our model could not follow Poisson distribution as there are no specific regions for irregularities since nodes keep on moving.

B. Rushing attack

For Rushing attack, every node keeps a count of requests received from the other node. For a node, out of total requests, majority requests are received from the same node, that node is culprit of flooding traffic and hence blacklisted by that node only. For Majority counting, we apply the arithmetic - divide total number of requests by two. If any node has generated requests greater than or equal to this, that node is forming rushing attack.

C. Decoy attack

For Decoy attack, node is offered data or service. Offline rating is done for the data and service. We follow majority model. A particular node in consideration has provided wrong data or poor service for more than half of the service request, that node is forming Decoy attack.

All student nodes who have enrolled for the course start with the trust score of 0.5.

We use ns3 to simulate university working day scenario in the information technology department. The model presents the everyday timetable of postgraduate students who attend classes, laboratories, tutorials and often go to the canteen, take part in events or go out for work. Our goal is to compute trust over time and also to show the general feasibility of our approach i.e. it is extended for undergraduate students comprising the strength of 120 students and then for the whole college and university.

While setting the parameters for linear increment/decrement we wanted to keep the punishmen/reward to be low. We tried the simulation with values in the range of 0.01 to 0.4. We observed that the transformation was frequent between node being blacklisted to node allowed for communication if the values are in the range of 0.1 to 0.4 and vice versa. We tried the linear decrement (0.01,0.02,0.03,0.04,0.05,0.06,0.07). For longitivity factor we had 3 situations

{node in neighbourhood,valid lifetime},
{node in neighbourhood,invalid lifetime},
{node not in neighbourhood,invalid lifetime}.

Node can be in either situation and probability is equal.So longitivity factor is set to 0.33.While setting the weight, we wanted w_p, w_{ss} to play significant role so we kept it high 0.9,0.8 but w_{js} is 0.5 so this opinion cannot rule the opinions with weights w_p, w_{ss}. We kept w_p,w_{ss} to {0.8,0.7},{0.7,0.6} but found that this weights intermixed with each other and their significance is not retained.
We evaluated following scenarios.

1) When a new “not enrolled student” enters, Professor node does a handshake process to establish trust.
2) Node 7 is dropping the packets.
3) Node 4 is giving false criticism.
4) Node 9 is giving false praise.

TABLE IV. Simulation parameters

NOTATION	PARAMETERS	VALUES
x	Longitivity Factor	0.33
η_d	Decrement Factor	0.01
η_{ib}	Increment Factor(belief)	0.02
η_{id}	Increment Factor(disbelief)	0.01
N	Netwrok Size	19
N_s	Total Transactions	1000
LC_s	Local Table Update Time	Each Transaction
GC_s	Global Cycle Time	120 minutes

M	Mobility Model	CONSTANTPOSITION MOBILITYMODEL(100)

TIs	Total Iteration Cycle	8 Days
w_p	Weight of Highest Category Node	0.9
w_{ss}	Weight of Intermediate Category Node	0.8
w_{js}	Weight of Lowest Category Node	0.5
α	Adjustment Factor	0.59

It is observable that overall more than 50 transactions occur per day. It is observable that 10% nodes are malicious either dropping packets or propagating false praise or false criticism. 10% nodes are inactive – not participating. 80% nodes are behaving properly. During the specific timetable schedules of the course, communication rate is high. In free time, the nodes move around so communication rate is low. We further evaluate trust score and observe that the consensus operator provides perfect protection against false praise and false criticism attack. Node 2 is a good node but it has been a victim of false criticism. We show how consensus operator neutralizes false criticism effect. At the end of 5 days trust score stabilizes. We observe the trust value for the nonparticipating node.

Message overhead in communication:In frMANET, the message overhead is affected by network size and the amount of data exchanged. The topology has no significant role to play.frMTP considers only randomly chosen two nodes to compute global trust, the message overhead is manageable. The observation is when students are moving in group, group communication(only one node in group) communicates with one node in other group. At time=380 seconds, the experiment observes the lowest communication message overhead in students movement trace. The conclusion is that outside the class, students move in clusters so only one member is communicating to other cluster and passing the supplied information to the whole group(cluster). A number of average messages exchanged decreases in group communication.

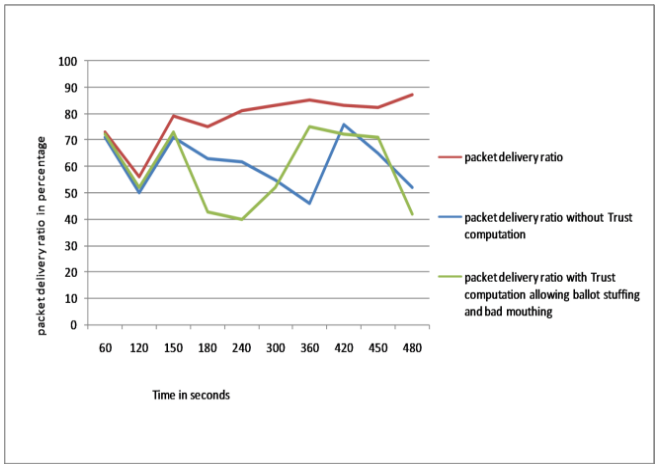

Fig. 1. Packet delivery ratio

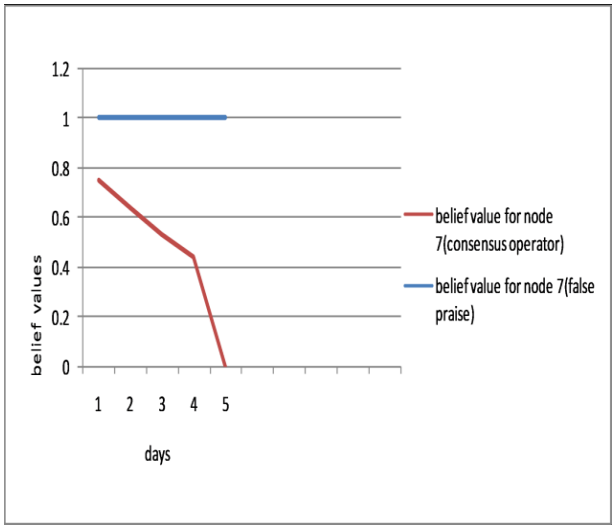

Fig. 2. Belief value computation(counterfeiting ballot stuffing)

TABLE V. BELIEF VALUE(FALSE CRITICISM)

Day	Belief value for node 2 (with consensus operator)	Belief value for node 2(false criticism)
1	0.27	0
2	0.34	0
3	0.45	0
4	0.48	0
5	0.5	0

TABLE VI. LIFETIME EFFECT ON BELIEF VALUE

Time in seconds	Belief value
120	0.36
240	0.26
360	0.19
480	0.09

TABLE VII. Effect of η_d

Time in seconds	Belief value when η_d =0.01	Belief value when η_d =0.02	Belief value when η_d =0.03
1.2	0.7	0.7	0.7
1.25	0.69	0.68	0.67
1.3	0.68	0.66	0.64
1.35	0.67	0.64	0.61
1.4	0.66	0.62	0.58
1.45	0.65	0.6	0.55
1.5	0.64	0.58	0.52

1.55	0.63	0.56	0.5
1.6	0.62	0.54	0.47
1.65	0.61	0.52	
1.7	0.6	0.5	
1.75	0.59		
1.8	0.58		
1.85	0.57		

While simulating, node 2 wanted to send data to node 9. The path to node 9 was via node 8. Node 8 had fluctuating communication channel due to device problem. While establishing route, node 8 could respond. At the time of data transfer node 8 went out of order. So belief value had to be decremented.

We tried different decrement factors. Though node 8 never had malicious intensions, it could not take part due to network problem. We did simulation by keeping η_d = 0.01, η_d =0.02 η_d =0.03. We found that since node 2 wanted to send data to node 9 on priority, it kept on trying frequently. Everytime on failed delivery, node 8 lost belief value though it never had a bad intention of dropping the packet. Upon reaching the value below 0.5, node got blacklisted. The restoration of wireless network takes any random time. Hence we took η_d = 0.01, giving a genuine node benefit to slowly converge to black listed node.

TABLE VIII. Comparison of our system with other trust based system

Comparison parameter	Buchegger et al.[2]	cTrust[3]	Credence[5]	Qin et al.[15]	Our approach
Bootstrapping	Not defined.	Not defined	Not defined	New node is assigned neutral reputation value. Nodes frequently communicate with one another	New node is assigned a lowest threshold value that allows node to participate.
Trust Evidence	Distributed approach. Promiscuous mode. Node listens to the traffic.	Aggregation of trust values.	Voting based	Central authority calculates trust based on direct observations.	Distributed approach. Local and global trust values will be computed.
Digital signature for nonrepudiation	Not present	Not present	Not present	Not present	RSA based PKI with 16 bit key for ease of computation. Key changes at regular interval.
Trustworthiness Evaluation	Beta distribution. More weight to first hand observation then second hand observations.	Probability based model	Manual	Beta distribution with more weight to past observations.	Subjective logic based. Consensus for parallel paths and discounting for transitive paths.
Trust aware interaction decisions	Threshold based and weight based.	Threshold based	Manual	Threshold based and weight based.	Threshold based and weight based.
Interaction outcome evaluation	Weighted sum is used to detect malicious nodes	Cumulative rating of the whole path.	Cluster based. Correlation values are established.	Weighted average sum is used to identify the malicious node.	Weighted sum of randomly chosen 2 nodes are considered to blacklist the node.

V. CONCLUSION

In this paper, we have proposed the trust model for information sharing among nodes in MANET with fixed and random movement based on subjective logic and peer's collaborations including collaboration in routing and service providing. We observed that for our simulation trace most of the nodes helped in routing but not collaborative in service providing. Initially, our scheme gives 50-70% packet delivery ratio, same as if trust based computation is not applied or trust computation is affected by ballot stuffing or bad mouthing. Once our scheme has been applied iteratively, after 4 iterations packet delivery ratio is increased to 90%, the effect of ballot stuffing and bad mouthing is neutralized. The message passing increases overheads but relatively less burden in our scheme because of periodic message transfer.

The trust computation scheme is based on subjective logic operators that put less computational overhead on the node.

The scheme provides the foundation for designing trust enabled applications where fixed and random movements are considered.

FUTURE WORK

We have designed the approach that will be applied to a small group. In future the scheme can be worked out for large group.Optimization of data structure for storing local values can be done using tree structure. This scheme is tested for AODV, for other routing protocols, the scheme can be tested.

REFERENCES

1. D. Ganesh and M. Sirisha, "Reputation and Trust Evaluation in MANETs Using Eigen Trust Algorithm", VSRD-IJCSIT, vol. 2, no. 3, pp. 175-189, 2012.
2. S. Buchegger and J.-Y. L. Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", Technical Report (IC/2003/50),EPFL-IC-LCA, Lausanne, Switzerland,2003.
3. Zhao H.,Yang X. and Li X., "cTrust:Trust Management in cyclic Mobile ad hoc networks", IEEE transaction vehicular technology, vol 62, pp. 2792-2806, Jul 2013.
4. Ayday E., Lee H. and Fekri F., "An iterative algorithm for Trust management and adversary detection for delay tolerant networks",IEEE transactions on mobile computing, vol 11, no.9, pp. 1514-1531, Sept 2012
5. Walsh K. and Sirer E., "Experience with an Object Reputation System for Peer-to-Peer File sharing", In proceedings of the Symposium on Network System Design and Implementation, San Jose, USA,2006.
6. Zhou L. and Haas Z., "Securing Ad Hoc Networks", IEEE Network, vol. 13,no. 6,pp. 24-30, Nov/Dec 1999.
7. Zhang Y. and Lee W., "Intrusion Detection in Wireless Ad-Hoc Networks", In Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, pp. 6-11, Aug 2000.
8. Shillo M., Funk P. and Rovatsos M., "Using trust for detecting deceitful agents in artificial societies", Applied Artificial Intelligence, vol.14, no.8, pp. 825-48, Sept 2000.
9. Warne D.and Holland C., "Exploring trust in flexible working using a new model", BT Technology Journal, vol.17, no.1, pp. 111-19, Jan 1999.
10. Josang A.,Bhuiyan T.,Xu Y. and Cox C., "Combining Trust and Reputation Management for Web-Based Services", In proceedings of 5th International Conference on Trust, Privacy & Security in Digital Business (TrustBus2008), Turin, Sept 2008.
11. Josang A., "An Algebra for Assessing Trust in Certificate Chains", In Proceedings of NDSS'99, Network and Distributed System Security Symposium, The Internet Society, San Diego, USA,1999.
12. Josang A., Hayward R. and Simon P., "Trust Network Analysis with Subjective Logic", In proceedings of 29th Australasian Computer Science Conference (ACSC2006), Hobart, Tasmania, Australia, January 2006.
13. Josang A., "Trust and reputation systems", tutorial at IFIPTM 2009, Purdue University, Jun 2009.
14. Feng L.and Jie W. "Uncertainty modeling and reduction in MANETS", IEEE transactions in mobile computing, vol 9, pp. 1035-1048, July 2010
15. Singh A.,"Role based trust management security policy analysis", International Journal of Engineering Research and applications, vol 2,Issue 6, November-December 2012
16. Rajaram A. and Palniswami S., "A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009
17. Jabbehdari S., Sanandaji A. and Modiri N. , "Evaluating and Mitigating the Effects of Selfish MAC Layer Misbehavior in MANETs", Journal of computing, volume 4, issue 2,Feb 2012.
18. Buchegger S. and Boudec J.-Y. Le, "A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks" In Proceedings of P2PEcon 2004, Harvard University, Cambridge MA, U.S.A., Jun 2004.
19. Hu, J. and Burnmester, M., "LARS: a locally aware reputation system for mobile ad-hoc networks", In 44th annual ACM Southeast Regional Conference,2006.
20. Chen A., XU G. and Yang Y., "A Cluster Based Trust Model For Mobile Ad-hoc Networks", 4th International conference on wireless communications, Networking and mobile computing , Wicom '08, 2008.
21. Pirzada A.,McDonald C. and Datta A., "Dependable Dynamic Source Routing without a Trusted Third Party".In proceedings of 28th Australasian conference on Computer Science, Newcastle, Australia, pp. 79-85,2005.
22. Dalal R., Khari M. and Singh Y, "Different Ways to Achieve Trust in MANET", International Journal on AdHoc Networking Systems (IJANS), Vol. 2, No. 2, pp. 53-64,Apr 2012.
23. Felix G. and Gregorio M., "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems", Computer standards and interfaces, Vol. 32(4), pp. 185-196, February 2010.
24. Yu H., Shen Z.,Miao C., Leung C. and Niyato D.,"A Survey of Trust and Reputation Management Systems in Wireless Communications", In proceedings of the IEEE, vol. 98, no. 10,pp. 1755-1772,Oct 2010.
25. Pirzada A. and McDonald C., "Trust Establishment In Pure Ad-hoc Networks", Wireless Personal Communications, Springer, vol. 37, pp. 139–163,2006.
26. Zakhary S. and Radenkovic M.," Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments" In proceedings of seventh international conference on Wireless On-demand Network Systems and Services (WONS), Kranjska Gora, Slovenia,2010.
27. Manan J., Bakar A. and Ahmad A.,"Trust formation based on subjective logic and PGP web-of-trust for information sharing in Mobile Ad-Hoc Network", In proceedings of IEEE International Conference on Privacy, Security, Risk and Trust,pp. 1004-1009,2010
28. Mármol F. and Pérez G.,"Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems", Computer Standards & Interfaces,vol. 32,pp. 185–196,2010

AUTHORS PROFILE

Dr. Hiteishi Diwanji, is an associate professor in L.D.College of Engineering. The area of interests are information security and wireless communication. The author has authored a book on "Computer programming and utilization". The author has prepared lectures in the area of information security for EPGPathshala.