Objective: This chapter defines trust, also describes properties and scope of trust. Different trust computation engines are described and their comparison is done. Subjective logic is described in detail. The chapter also describes Markov, Statistical, and Mobility Models.

3.1 Need of Trust based system

Trust and reputation management schemes are emerging as important decision tool in MANET. This helps in decision that which nodes in MANETs must be used for forwarding packets to other nodes, or for accepting information or services from other nodes. This decision making provides MANETs security from internal attacks where cryptographic security cannot work. Forming a mobile ad hoc network of nodes for routing and data sharing has been useful. This involves minimum efforts to set up the network. Trust is crucial as it helps in decision making. Trust helps in deciding whom 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 providing the file which is asked 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. Trust computation engine, in that case, decreases the trust and most trustworthy node is identified as a malicious node. In that case, communication will be done through less trustworthy nodes or no communication path can be found. To avoid this problem, we have considered node state while computing trust so no unnecessary decrement of trust values occur. Trust computation schemes are often the victim of false praise and false criticism leading to wrong trust value ending up in untrustworthy paths. Often node denies that it is falsely praising or falsely criticizing the other node.
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. Trust and reputation systems are emerging as important decision support tools for selecting the node for routing as well as getting services.

3.2 Definition of Trust

“Evaluation Trust” is the term defined by Gambetta. Evaluation Trust is the subjective probability for individual B assigned by an individual, A, thinking that, given action is performed by B on which its welfare depends.

“Decision Trust” is the term defined by McKnight &Chervany which emphasizes on willingness with sense of relative security so that dependence on someone else in a well defined situation can be made but it is possible that negative results can be obtained. Trust is derived from the reputation of the system.

Josang in [10] defines aspects of trust that includes scope of trust, functional trust, referral trust, direct trust and indirect trust. Scope of trust “σ” is attached to relying party and relying party is dependent on this function and also trusts this function. In case of Functional trust “fσ”, the trusted party executes the function. Referral trust “rσ” means recommending someone(a party) by trusted party that in turn performs the required. Direct trust “dσ” is derived from direct experience. The trust gathered from participants which is computed from recommendations is called Indirect trust “iσ”.

Trust measure μ can be defined in different ways.

a.) Binary (Trusted, not trusted),
b.) Discrete(strong, weak, trust, distrust),
c.) Continuous (percentage, probability, belief).
Definition of Trust

Time stamp is the time when trust was computed and expressed. It is denoted by Time \( \tau \). Trust is always the function of time and it diminishes with time.

Discrete binary form is used to express Binomial Bayesian reputation systems. Discrete binary form suggests that rating is - positive \((good)\) or negative \((bad)\). Discrete graded levels are used for Multinomial Bayesian reputation systems. Ratings are given with discrete graded levels such as mediocre - bad - average - good – excellent.

To establish Trust is a challenge. It is an important issue in case of secure routing for ad hoc networks. The infrastructure less nature of MANET and multi hop routes need trusted path to ensure packet delivery in the presence of intermediate malicious nodes. In MANET retransmission of packets is difficult and packet loss is intolerable. A trust model helps in establishing trusted paths and in turn increases packet delivery ratio. Trusted path ensures that node gets the service which it has asked for.

3.2.1 Trust scope

For relying party needs to decide, who to trust. For that trust scope is defined. And it is referred by the relying party.

- **Functional trust**: The trusted party performs the function. On the basis of that trust values are derived. It depends whether function performed successfully or not.

- **Referral trust**: To perform certain function, the trusted party gives recommendations for a party (who recommends a party) and then that party performs the function.

- **Direct trust**: Direct trust is the result of direct experience.

- **Indirect trust**: Indirect trust is the result computed from recommendations from others.

3.2.2 Properties of Trust

Following properties can be seen in the trust metric.

- Context dependence: Specific context is given in which the trust relationships are meaningful.

- Function of uncertainty: The said entity may perform assigned action with certain probability. Trust is an evaluation of that probability.
Trust Computation

Quantitative values: Trust can be represented as numeric value, continuous or discrete values.

Asymmetric: Even if A trusts B, not necessarily B trusts A. This proves that Trust is not identical in both directions proving that it is not necessarily symmetric.

Transitive: Trust is abided by transitive property. In case, node A trusts node B and node B trusts node C, then node A trusts node C. Though in reality it may differ, if A trusts B, and B trusts C, it does not guarantee that A trusts C. Trust is not perfectly transitive in a mathematical sense but personalized: Trust is inherently a personal opinion. Two people have different opinions in case of evaluation of trustworthiness about the same entity.

3.2.3 Reputation and trust-based systems can be broadly classified by the following groups:

3.2.3.1 Observation:

- First-hand: To update or establish trust, direct observation is used means system uses its own experience.

- Second-hand: To update or establish trust, the system uses information provided by participants.

Majority of the schemes derived till now are working on first-hand as well as second hand information and update reputation score. In such schemes opinion is built based on the knowledge gained from neighbors. Few systems do not rely on the both types of information. In case of the systems that use only first-hand information, other nodes do not influence the computation of the node’s reputation value. These schemes make the system robust against false opinions, but at the same time only first-hand information is not enough to build reputation of any particular node.

3.2.3.2 Information Symmetry
Symmetric: All nodes in the network have access to the same amount of information, i.e., both first-hand and second-hand. When making a decision, no node has more information than any other node. [12]

Asymmetric: All nodes do not have access to the same amount of information.

3.2.3.3 Centralization

Centralized: One central entity maintains the reputation of all the nodes in the network. Such a reputation system can cause both a security and information bottleneck.[12]

Distributed: Each node maintains the reputation information of all the nodes it cares about. In this kind of a reputation system, there could be issues concerning the consistency of reputation values at different nodes, i.e., there may not be a consistent local view. Each node can have either local or global information.

Local: Nodes have reputation information only of nodes in their neighborhood. This is the most reasonable option, particularly for static sensor networks, since nodes interact only with their immediate neighbours. This mitigates memory overhead to a large extent.

Global: Nodes have reputation information of all the nodes in the network. This is suitable for networks with lots of node mobility. Even after moving to a new location, nodes are not completely alienated and have a reasonable understanding of their new neighborhood. Unfortunately, this leads to a large overhead, and can lead to scalability problems.
Li and Singhal in their study compared trust management system that is either evidence-based or monitoring-based trust management. Nodes establish trust relationships. Any proof (evidence) that makes base for trust relationships among nodes is element of Evidence-based trust management: the proof elements include public key, address, identity. The proof element (evidence) can be generated using a challenge and response process that is used by any node for itself or for other node too. Monitoring-based trust management relies on direct information and based on that the trust level of each participating node is determined (e.g., observing the benign or malicious behaviors of neighboring nodes, such as packet dropping, and packet flooding leading to excessive resource consumption in the network, or denial of service attacks) as well as indirect
information (e.g., reputation ratings, means recommendations put forwarded from other nodes)

Aivaloglou et al. classify certificate-based framework and behavior-based framework, two types of trust building frameworks for MANETs. In the first, nodes are occupying predefined positions. Defined mechanisms work on that knowledge to populate trust relationships within the network. Nodes themselves or in cooperation with other nodes derive trust relationships using certificates. When certificates are used, they have to be distributed to all, maintained by particular node and managed by all. Trustworthiness of the target node is decided based on a valid certificate. Based on certificates trust decisions can be made. The certificates are either issued by certificate authority or by other nodes called the certificate issuer nodes. In behavior-based framework, all behaviors of neighbors are continuously monitored by each node and trust is computed. In the behavior-based framework reactive approach is followed, which assumes that the preloaded authentication mechanisms check the identities of nodes in the network. For example, the mechanism will prove a node to be a selfish node, if a node uses network resources in an unauthorized way and will be put up as in isolation from other nodes.

Aivaloglou et al.[36] also classify based on the kind of architecture used to establish trust: hierarchical framework versus distributed framework. In the first type of architecture, capabilities or levels of trust are used, based on that hierarchy is derived for the given group of nodes. In this framework, on line or off line evidence is provided by centralized certificate authorities or trusted third parties. Distributed nature of systems does not support centralized infrastructure; so in distributed environment, all nodes have few and equal, responsibility for acquiring, maintaining, and later on distributing trust evidence.

3.3 Trust Computation Engines

3.3.1 Summation and average

In case of summation and average, the equation is given by

\[
\text{Summation Reputation score} = \Sigma(\text{positive}) - \Sigma(\text{negative})
\]

\[
\text{Average Reputation score} = \frac{\Sigma(\text{ratings})}{N(\text{ratings})}
\]
Summation Reputation score is used by Ebay and average reputation score is used by Epinions. This model can be combined with sliding time windows. Though the method is very easy from the understanding and implementation view but the results may not be accurate, generating the false values of reputation.

### 3.3.3 Hidden Markov Model

In this model true nature of future services are unknown. This models work on States of service where Service provider is modeled as a Markov chain. This model is sound statistically but parameters are required.

### 3.3.4 Bayesian Reputation Systems

This flow model is theoretically well proven algorithm for rating and includes models based on Binomial and multinomial functions. Rating does not have range bounds in this model. The operators used are combination, discounting. Longevity factor is considered with weight ~ transaction value.

#### 3.3.4.1 Binomial reputation Computation considering longevity factor

The following parameters are considered.

- \( R_i \): collected positive evidence at time \( i \)
- \( S_i \): collected negative evidence at time \( i \)
- \( r \): positive evidence considering unit time interval
- \( s \): negative evidence considering unit time interval
- \( \lambda \): longevity factor in range \([0,1]\)

\[
R_{i+1} = \lambda \cdot R_i + r_i \text{: Recursive updating algorithm}
\]

\[
S_{i+1} = \lambda \cdot S_i + s_i \text{: Recursive updating algorithm}
\]

Score calculation is done according to following equation.

\[
Score \; \text{SCORE}_i = \frac{r_{base_i} + R_i}{r_{base_i} + s_{base_i} + R_i + S_i} \text{ : Score at time period } i
\]

Typically, \( r_{base} = 1, s_{base} = 1 \)  

#### 3.3.4.2 Multinomial reputation score:

\[ \tilde{a} \cdot r \]
The multinomial reputation score follows the Dirichlet-PDF probability expectation. The computation engine needs following

1) Reputation score
2) Multinomial evidence vector
3) Multinomial base rate vector

\[ W = 2 \quad \text{Weight of non-informative prior} \]

\[ l: \text{Number of rating levels} \]

\[ L_j: \text{particular rating level} \]

\[
\text{Score}(L_j, \bar{R}, \bar{a}) = \frac{R(L_j) + W \cdot a(L_j)}{W + \sum_{j=1}^{l} R(L_j)}
\]  

(2)

3.3.4 Discrete Models

Discrete measures are categorized as “Very trustworthy”, “trustworthy”, “untrustworthy” Computation. This uses Heuristic formula for computation or use lookup tables. The model is easy to understand, qualitative but if theoretically considered than does not give concrete base.

3.3.5 Belief models

This model starts working with assumption of a trust scope \( \sigma \).

a.) Each trust scope has two semantically differing variants.

Functional: Trust x for scope \( \sigma \). Asking for water tap fitting, one need to rely on plumber so function of fitting water tap will define a plumber to be good or not.

Referral: Trust x to refer or recommend someone/thing for scope \( \sigma \). Someone has got a good work done from a plumber so he will recommend that plumber as a good plumber.

b.) There are two topological types.

Direct: Direct experience has helped in establishing Trust.

Indirect: Trust is derived as a result of second hand evidence.

3.3.6 Flow models

a. This model performs Transitive iteration through graph. This model can have Loops and arbitrarily long paths.
b. Uniform Distribution of Source who provides trust. Early version of PageRank had uniform distribution. Sources are distributed discretely, as in current PageRank and EigenTrust. In this model Sum of trust can be constant, e.g. PageRank or increasing with network size, e.g. EigenTrust

We evaluated all trust computation engines. 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 pre specified because of the dynamic nature of MANET. Discrete models, flow models and fuzzy models do not provide relevant mathematical background for trust calculation in MANET. Bayesian Reputation Systems are widely used in literature but they do not consider uncertainty. Nodes inherently involve uncertainty in the behavior so we considered belief model based on subjective logic.

### 3.4 Subjective Logic

When standard logic is considered, propositions are evaluated to produce either true or false. Probabilistic logic considers the range [0,1] to express the arguments as a probability. Degrees of uncertainty is involved in Subjective logic which otherwise is a probabilistic logic where degrees of uncertainty are used to express probability values. There is a bijective mapping that exists between respective trust and reputation representations meaning Trust models derived based on subjective logic and Bayesian reputation systems are directly compatible. Subjective logic is generalization of binary logic and probability calculus.

- Probability calculus –Probability calculus is considered to be dogmatic opinions where $u_x=0$ which is equivalent to probabilities.
- Binary logic –Binary logic is considered to be absolute opinions $b_x=1$ which is equivalent to TRUE.
- Subjective logic that considers uncertainty is also a probabilistic logic. This considers uncertainty explicitly. Ownership means one who has derived this belief.
- Arguments are passed to subjective logic, if proposition is considered then they are subjective opinions about proposition.
- Binomial subjective opinions is given by
  - $b^A_x = b(x)$ where $A$'s belief in $x$
  - $d^A_x = d(x)$ is observer $A$'s disbelief in $x$
Subjective Logic

- $u_x^A = u(x)$ is observer A’s uncertainty about x
- $a_x^A$ is the base rate of x
- b,d,u represent belief, disbelief, uncertainty respectively where $b,d,u \in [0,1]$ and $b+d+u=1$.
- Base rate is the default value if belief value is yet not computed.
- The confidence parameter can be defined as equal to $(1-c)$. The confidence of a trust value is equal to the certainty of the corresponding opinion.
- Probability Expectation value $E(w) = b+au$
- The probability density over binary event spaces can be expressed as beta PDFs (Probability Density Functions) denoted by beta($\alpha, \beta$). r and s express number of positive and negative past observations respectively.
  \[
  \alpha = r+2a \\
  \beta = s+2(1-a) \tag{3}
  \]

In probabilistic logic, and binary logic, it is difficult to express degrees of ignorance present in case of input arguments. Consider the expression “I don’t know”, it cannot be expressed. Even if analyst is not able to provide any reliable value for the given input argument, a value has to be set. This leads to unreliable conclusions, in literature it is described as the “garbage in - garbage out” problem. For the expression, “I don’t know the truth values of $x_1$ and $x_2$” and the analyst needs to derive $p(x_1 \land x_2)$, then there does not exist anything in probabilistic logic. Even Kleene’s three-valued logic does not provide an adequate model. Kleene’s logic dictates value UNDEFINED for $(x_1 \land x_2)$ when $x_1$ and $x_2$ are defined as UNDEFINED. In case of an arbitrarily large number of variables $x_i$ that are all UNDEFINED, the model hangs. Arguments in subjective logic form subjective opinions about propositions. Consider single proposition, where a binomial opinion is applied, and can be represented as a Beta distribution. In case of multinominal opinion, a collection of propositions are applied, and can be represented as a Dirichlet distribution.

Subjective logic defines a trust metric called opinion denoted by $w_x^A = (\tilde{b}, u, \tilde{a})$, which expresses the relying party A’s belief over a state space X. Here $\tilde{b}$ represents belief masses over the states of X, and u represent uncertainty mass where $\tilde{b}, u \in [0, 1]$ and $P(\tilde{b} + u) = 1$. The vector $\tilde{a} \in [0, 1]$ represents the base rates over X, and is used for computing the probability expectation value of a state x as $E(x) = \tilde{b}(x) + \tilde{a}(x)u$, meaning that
Trust Computation

\[ \tilde{a} \] determines how uncertainty contributes to \( E(x) \). Binomial opinions are expressed as \( w_{x}^{A} = (b, d, u, a) \) where \( d \) denotes disbelief in \( x \).

When trust and referrals are expressed as subjective opinions, each transitive trust path Alice→Doll→James, and Alice→Clerk→James can be computed with the transitivity operator, where Doll and Clerk both refer to James. The reference trust is discounted as a function Alice’s trust in Doll and Clerk respectively. Cumulative or averaging fusion operator is used to combine two paths.

\[ [A:B] \] denotes a trust relationship between \( A \) and \( B \). “:\)” symbolizes the transitivity of two arcs and “\( \diamond \)” symbolizes the fusion of two parallel paths. “\( \otimes \)” corresponds transitivity operator for opinions and “\( \oplus \)” denotes fusion operator.

3.4.2 Binomial Opinions

3.4.2.1 Binomial Opinion Representation

Binomial opinions are expressed over binary frames, and their mathematical representation is done by a special notation. To consider general \( n \)-ary frame \( X \) as a binary two situations are taken. a binary partitioning consisting of (i) one of its proper subsets \( x \) and (ii) the complement \( x \).

**Definition 1 (Binomial Opinion)** Let \( X = \{ x, \overline{x} \} \). \( n \)-ary frame can be a binary frame or a binary partition. Quadruple \( \omega_{x} = (b, d, u, a) \) is a binomial opinion about the truth of state \( x \) is the ordered where:

- \( x \) is true then belief mass in support is \( b \) (belief)
- \( x \) is false then belief mass in support is \( d \) (disbelief)
- belief mass is not committed then \( u \) (uncertainty),

In the absence of committed belief mass \( a \) (base rate) is the a priori probability.

These components satisfy \( b + d + u = 1 \) and \( b, d, u, a \in [0, 1] \). There are different binomial opinion classes with different characteristics. A binomial opinion:

Where \( b = 1 \) is equivalent to binary logic TRUE,
Where \( d = 1 \) is equivalent to binary logic FALSE,
where \( b + d = 1 \) is equivalent to a traditional probability,
where \( b + d < 1 \) expresses degrees of uncertainty, and
where \( b + d = 0 \) expresses total uncertainty.

The probability projection of a binomial opinion on proposition \( x \) is defined as
Subjective Logic

3.4.2.2 The Beta Binomial Model
A Beta pdf (probability density function) is symbolized as $Beta(p | \alpha, \beta)$. $\alpha$ and $\beta$ are its two evidence parameters, a general Binomial opinion with uncertainty corresponds to where Beta pdfs are expressed as:

$$Beta(p | a, b) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{a-1} (1 - p)^{b-1}$$ (4)

Where $0 \leq p \leq 1$, $\alpha > 0$, $\beta > 0$, with $p \neq 0$ if $\alpha < 1$, and $p \neq 1$ if $\beta < 1$. $p$ has this restriction which is a probability variable.

For $x$, Let $r$ is the number of good observations, and let $s$ is the number of bad observations. Considering base rate $a$, the $\alpha$ and $\beta$ parameters can be expressed as a function of the observations $(r, s)$.

$$\alpha = r + Wa$$
$$\beta = s + W(1 - a)$$

$$Beta(p | r, s, a) = \frac{\Gamma(r + s + W)}{\Gamma(r + Wa)\Gamma(s + W(1 - a))} p^{(r+Wa-1)} (1 - p)^{(s+W(1-a)-1)}$$ (5)

where $0 \leq p \leq 1$, $(r + Wa) > 0$, $(s + W(1 - a)) > 0$, is other presentation for the above equation where probability variable $p \neq 0$ if $(r + Wa) < 1$, and $p \neq 1$ if $(s + W(1 - a)) < 1$ that is the restriction on $p$.

$W$ indicates the non-informative prior weight. $W=2$ normally, that ensures that the base rate $a = 0.5$ by default when no prior (i.e. when $r = s = 0$) observations are available. The Beta pdf with default value is shows behavior of a uniform pdf.

The probability expectation value of the Beta pdf is defined below:

$$E(Beta(p | a, b)) = \frac{\alpha}{\alpha + \beta} = \frac{r + Wa}{r + s + W}$$ (6)

3.5 Opinion Classes with their representation
3.5.2 Binomial Opinion with corresponding Beta Mapping
Let a binomial opinion be \( \omega_x = (b, d, u, a) \). The parameters of a Beta pdf is denoted as \( \text{Beta}(p \mid r, s, a) \). Their mapping is as follows:

**Definition 2 (Binomial Opinion-Beta Mapping)**

Let a binomial opinion be \( \omega_x = (b, d, u, a) \) and for the same proposition \( x \) let \( \text{Beta}(p \mid r, s, a) \) be a Beta pdf, or similarly, the binary state space be \{x, \overline{x}\}. The equivalency of opinions \( \omega_x \) and \( \text{Beta}(p \mid r, s, a) \) is as follows:

| \( b \) | \( \frac{r}{W + r + s} \) | \( r = \frac{WB}{u} \) | For \( u \neq 0 \) |
| \( d \) | \( \frac{s}{W + r + s} \) | \( s = \frac{Wd}{u} \) | For \( u = 0 \) |
| \( u \) | \( \frac{W}{W + r + s} \) | \( 1 = b + d + u \) | |

**Theorem 1. Equivalence Between Opinions and Reputations**

Let an opinion be denoted as \( \omega = (\tilde{b}, u, \tilde{a}) \), and Reputation be denoted as \( \tilde{R} \). Let the state space be \( X \), both opinion and reputation are defined over \( X \) where the base rate \( \tilde{a} \) also applies to the reputation. Then the following equivalence holds [3]:

For \( u \neq 0 \):

\[
\tilde{b}(x_i) = \frac{\tilde{R}(x_i)}{C + \sum_{i=1}^{k} \tilde{R}(x_i)} \quad \text{and} \quad \tilde{R}(x_i) = \frac{C\tilde{b}(x_i)}{u}
\]

\[
\begin{align*}
\text{For u=0:} \\
\tilde{b}(x_i) &= \eta(x_i) \\
\tilde{R}(x_i) &= \eta(x_i) \sum_{i=1}^{k} \tilde{R}(x_i) = \eta(x_i) \infty
\end{align*}
\]
Degree of uncertainty is always used to express Subjective opinions. Subjective opinion expresses beliefs about the truth of propositions, and Ownership of the opinion is also indicated whenever necessary. \( w^A_x \) expresses a subjective opinion where \( A \) is the one who gives opinion, is said to be subject, and opinion is applicable to the target frame \( X \). \( \omega(A : X) \) is the other way to express opinion.

An opinion has optional attributes the belief owner (subject) and the propositions (object). The belief vector \( \vec{b}_X \), the uncertainty mass \( u_X \) and the base rate vector \( \vec{a}_X \) forms a composite function that builds an opinion.

There are particular classes of opinions. If opinion is binomial, it is applied on binary frames. Uncertainty classifies the opinions. For uncertain opinion, \( u_X > 0 \). Dogmatic opinion is one when \( u_X = 0 \).

Table 3.1 Opinion classes with equivalent probabilistic representation

| Opinion Class          | Binomial Cardinality \(|x|=2\) | Multinomial Cardinality \([X]>2\) |
|------------------------|---------------------------------|----------------------------------|
| Uncertain \( u>0 \)    | UB opinion Beta pdf             | UM opinion Dirichlet pdf over X  |
| Dogmatic \( u=0 \)     | DB opinion Scalar probability   | DM opinion Probabilities on X    |

Table 3.2 Correspondence between probability, set and logic operators

<table>
<thead>
<tr>
<th>Subjective logic operator</th>
<th>Symbol</th>
<th>Binary logic/set operator</th>
<th>symbol</th>
<th>Subjective logic notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addition</td>
<td>+</td>
<td>Union</td>
<td>( \cup )</td>
<td>( w_{x+y} = w_x + w_y )</td>
</tr>
<tr>
<td>Subtraction</td>
<td>-</td>
<td>Difference</td>
<td>( \setminus )</td>
<td>( w_{x\setminus y} = w_x - w_y )</td>
</tr>
<tr>
<td>Multiplication</td>
<td>\cdot</td>
<td>AND</td>
<td>( \wedge )</td>
<td>( w_{x\wedge y} = w_x \cdot w_y )</td>
</tr>
<tr>
<td>Division</td>
<td>\div</td>
<td>UN AND</td>
<td>( \dot{\wedge} )</td>
<td>( w_{x\dot{\wedge} y} = w_x / w_y )</td>
</tr>
<tr>
<td>Discounting</td>
<td>\otimes</td>
<td>Transitivity</td>
<td>:</td>
<td>( w^A_X : B = w^A_b \otimes w^B_x )</td>
</tr>
<tr>
<td>Cumulative Fusion</td>
<td>\ominus</td>
<td>n.a.</td>
<td>( \diamond )</td>
<td>( w^A_X \diamond B = w^A_x \otimes w^B_x )</td>
</tr>
</tbody>
</table>

3.5.2 Generalizing Probabilistic Logic as Subjective Logic:
Binary logic TRUE or FALSE is the argument opinions; the corresponding propositional/binary logic operator gives the same result as the result generated by any of the subjective logic operator. When traditional probabilities are the bases of the argument opinions, corresponding probability operator generates the result same as any of the subjective logic operator.

When degrees of uncertainty is observed in the argument opinions, correct expectation value is derived from the operators involving multiplication and division which are derived opinions that always have but possibly with approximate variance when seen as Beta/Dirichlet probability distributions. Analytically correct values for the expectation value and the variance are always observed in case of all other operators.

3.6 Discounting operator

To compute transitive trust, Discounting is used. It is denoted by $\otimes$.

When transitive path is considered, Discounting increases uncertainty so that the expectation value in confidence is reduced.

3.7 Consensus operator

$$w_c^{A\otimes B} = w_c^A \oplus w_c^B$$

$$w_c^{A\otimes B} = \{ w_c^A \otimes w_c^B \}$$

$$w_c^{A\otimes B} = \{ b_c^{A,B}, d_c^{A,B}, u_c^{A,B}, a_c^{A,B} \}$$

$$b_c^{A,B} = b_b^A b_c^B$$
$$d_c^{A,B} = b_b^A d_c^B$$
$$u_c^{A,B} = d_b^A + u_b^A + b_b^A u_c^B$$
$$a_c^{A,B} = a_c^B$$

Case 1:

$$b_c^{A\otimes B} = \frac{b_c^A u_c^B + u_c^A u_c^B}{u_c^A + u_c^B - u_c^A u_c^B}$$
$$d_c^{A\otimes B} = \frac{d_c^A u_c^B + d_c^B u_c^A}{u_c^A + u_c^B - u_c^A u_c^B}$$
$$u_c^{A\otimes B} = \frac{u_c^A u_c^B}{u_c^A + u_c^B - u_c^A u_c^B}$$
$$u_c^{A\otimes B} = a_c^A$$
Case 2:

1. 
\[ u_c^A + u_c^B - u_c^A u_c^B = 0 \]
\[ b_c^{AB} = (\lambda^A b_c^A + b_c^B)/(\lambda^B + 1) \]  \hspace{1cm} (9)
\[ d_c^{AB} = (\lambda^A d_c^A + d_c^B)/(\lambda^B + 1) \]
\[ u_c^{AB} = 0 \]
\[ a_c^{AB} = a_c \]

2. 
\[ u_c^A = 0 u_c^B = 0 \]
\[ c_c^A = l c_c^B = 1 \]
\[ b_c^{AB} = (b_c^A c_c^A + b_c^B c_c^B)/(c_c^A + c_c^B) \]  \hspace{1cm} (10)
\[ d_c^{AB} = (d_c^A c_c^A + d_c^B c_c^B)/(c_c^A + c_c^B) \]
\[ u_c^{AB} = 0 \]
\[ c_c^{AB} = c_c^A + c_c^B \]
\[ a_c^{AB} = a_c \]

3. 
\[ u_c^A = 0 u_c^B = 1 \]
\[ c_c^A = l c_c^B = 0 \]
\[ b_c^{AB} = b_c^A \]  \hspace{1cm} (11)
\[ d_c^{AB} = d_c^A \]
\[ u_c^{AB} = u_c^A \]
\[ c_c^{AB} = c_c^A \]
\[ a_c^{AB} = a_c \]

4. 
\[ u_c^A = 1 u_c^B = 0 \]
\[ c_c^A = 0 c_c^B = 1 \]
\[ b_c^{AB} = b_c^B \]  \hspace{1cm} (12)
\[ d_c^{AB} = d_c^B \]
\[ u_c^{AB} = u_c^B \]
\[ c_c^{AB} = c_c^B \]
\[ a_c^{AB} = a_c \]
Consensus operator reduces uncertainty, i.e. increase the confidence in the expectation value.

### 3.8 Markov model

This represents a mathematical system that undergoes transitions from one state to another between a finite or countable number of possible states. Characterized as memoryless, this is a random process. The next state depends only on the current state and not on the sequence of events that preceded it.

### 3.9 Statistical Model

This model is a formalization of relationships between variables in the form of mathematical equations. A statistical model describes how one or more random variables are related to one or more other variables. In this model, the variables are not deterministically but stochastically related. A deterministic system is a system in which no randomness is involved in the development of future states of the system. A deterministic model will thus always produce the same output from a given starting condition or initial state.

In probability, a stochastic system is one whose state is nondeterministic. The subsequent state of a stochastic system is determined both by the system’s predictable actions and by a random element. A stochastic process is one whose behavior is nondeterministic. It is a sequence of random variables.

Nodes in MANET represents a statistical model as \((Y,P)\). \(Y\) is in packet forwarded, packet dropped, service provided, service not provided, service provided that is asked for, service provided with something other than what is asked for. The probability is between 0 to 1. In MANET the conclusions are drawn from data that is subject to random variation called statistical inference. The randomness is involved in movement and node’s own perspective in participating in group activity.
3.10 Mobility Models

a.) Random Walk Mobility Model (RWMM) – This model is memoryless mobility model. Current speed and direction is independent of past speed and direction. This can generate unrealistic movements such as sudden stops and sharp turns.
b.) Random Waypoint Mobility Model (RWMM) – This model includes pause times between changes in direction and/or speed. Node begins by staying in one location for a certain period of time. Choose a random destination and speed [minspeed, maxspeed]
c.) Random Direction Mobility Model (RDMM) – This model creates density wave. Clustering of nodes occurs in one part of simulation area.

3.11 Problem Statement

To generate trusted path in mobile ad hoc network, mask bad mouthing and ballot stuffing using discounting in transitive paths and consensus in parallel paths minimizing the exchange of opinions from nodes, achieve nonrepudiation through public key based digital signature and achieve increase in throughput.

3.12 Scope

- Simulation of ad hoc network by our own configured nodes and network parameters.
- Identification of misbehaving nodes.
- Bad mouthing and ballot stuffing masked with consensus and discounting operator.
- Blacklist the node to achieve higher throughput.
- Nonrepudiation

Assumption: The node entering the ad hoc network is an authentic node and has got authentication token to participate in the network.

3.13 Objectives

The overall objectives of our research are summarized as:

- Use of belief model based subjective logic to compute trust.
• Identify node behavior based on the stochastic parameter in routing (packet forwarding, packet dropping) and in providing service (file sharing, file downloading) using Markov model. Updating local node trust table based on current transaction and current trust values. Node must be neither burdened with keeping the history of behavior nor should have the overhead of message passing.
• Node is busy in high priority work. Hence do not participate in routing or service providing. The trust values are not updated hence avoid unnecessary zigzags in trust values of good node.
• Use discounting and consensus operator for eliminating bad mouthing and ballot stuffing.
• Attaching public key based digital signature to avoid nonrepudiation in case of bad mouthing and ballot stuffing where node is denying the fact that it is constantly sending positive or negative opinions.
• Computing the global trust values and updating each node with new trust values for nodes in the ad hoc network at regular time interval.
• Punish the misbehaving nodes by blacklisting and barring them from participating in the network and also from getting services from the network.
• Increase the throughput in terms of packet delivery ratio.

3.14 Research Methodology utilized for research work

a) Null Hypothesis: In case of fixed and random moving nodes in MANET, misbehavior in routing or service providing, decrease belief, aggregate belief values by taking opinions, blacklist the node if belief is below threshold value.
b) Research Hypothesis: In case of misbehavior in routing or service providing, decrease belief, aggregate values using subjective logic by taking opinions, blacklist the node if belief is below threshold value masking ballot stuffing and bad mouthing.