Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey

Kannan Govindan, *Member IEEE* and Prasant Mohapatra, *Fellow IEEE*

Abstract

Trust is an important aspect of mobile adhoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques suited for other networks. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node. In this work we present a detailed survey on various trust computing approaches that are geared towards MANETs. We highlight the summary and comparisons of these approaches. In addition, we analyze various works on trust dynamics including trust propagation, prediction and aggregation algorithms, the influence of network dynamics on trust dynamics and the impact of trust on security services.

I. Introduction

Distributed collaborations and information sharing are considered to be essential operations in the MANET to achieve the deployment goals such as sensing and event monitoring. Collaboration will be productive only if all participants operate in a trustworthy manner [1]–[3]. MANETs are usually deployed in harsh or uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no centralized control unit to monitor the node operations. These characteristics force a component node to be cautious when collaborating/communicating with other nodes as the behaviour of nodes change with time and environmental conditions. Therefore, establishing and quantifying behaviour of nodes in the form of trust is essential for ensuring proper operation of MANET. This is particularly important in large scale networks where highly heterogeneous entities participate and high level of collaborations are required e.g., tactical networks with ally nations and social networks [4]. Heterogeneity could be in terms of nodes' operations, sensing capabilities, and other related behaviour.

Trust system can also be used in assessing the quality of received information, to provide network security services such as access control, authentication, malicious node detections and secure resource sharing [5]–[8]. Therefore, it is important to periodically evaluate the trust value of nodes based on some metrics and computational methods.

Trust computations in static networks are relatively simpler because the trust value here changes mainly due to behaviour of nodes. After enough observations these behaviours are predictable. However, in MANET trust computations are challenging because:

- There could be different types of mobility in MANETs such as low mobility (human walking with sensors) or high mobility (mobility of sensors mounted on vehicle). The network composition may significantly change with time in an unpredictable manner due to this mobility. When the neighbour constantly changes, it becomes difficult to make observation and get enough opportunities for interactions to measure the trust. Information received from the MANET nodes are more valuable and trustworthy if they can be related to where and when the readings originated [9]. However, when

K. Govindan and P. Mohapatra are with the Department of Computer Science, University of California Davis, CA- 95616, Email: {gkannan, prasant}@cs.ucdavis.edu

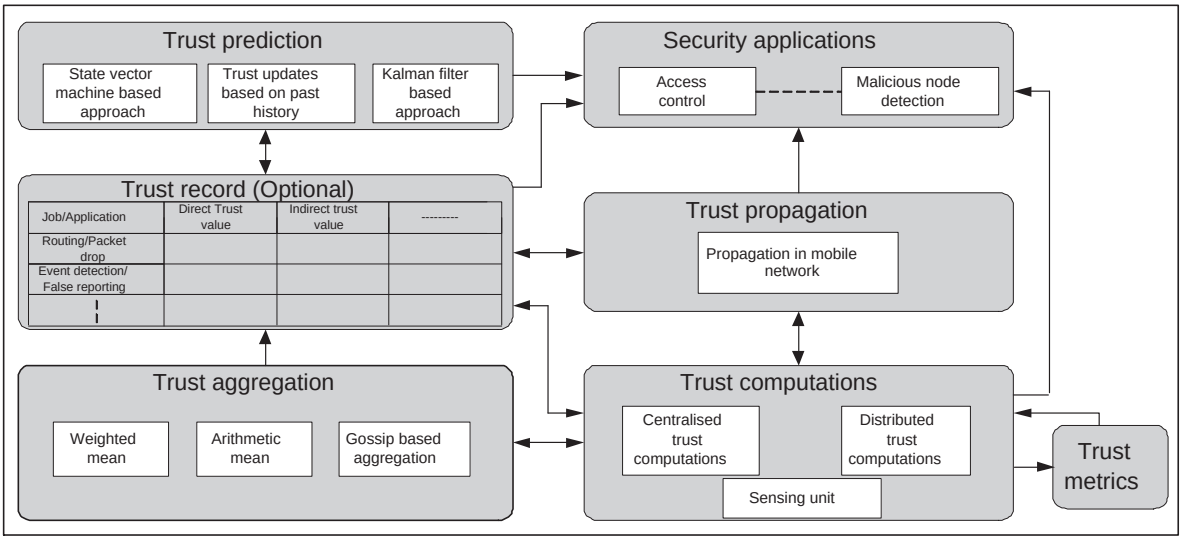


Figure 1. Relationship among various trust blocks

the location is constantly changing, it is hard to associate the information and node behaviour with locations.

- In the absence of centralized control station, monitoring the behaviour of nodes is very difficult. The complexity in trust computations grows non-linearly without the centralized command center. The worst case complexity of obtaining the trust level on every node by every other node in a network of N connected nodes is $O(N^2)$ [10].

Recently there has been much effort on various trust computing techniques with respect to MANET. A detailed survey and summarization of these techniques are necessary for trust system designer to understand the intrinsic of this domain.

There are some literature surveys available on trust in wireless sensor networks, social networks, internet applications and cognitive networks [11]–[19]. Nevertheless, exhaustive/cohesive surveys handling MANETs are still lacking. There is a recent survey on trust management for MANET in [20]. However, this paper mainly handles various trust management issues including metrics, attack models on trust management and applications. The detailed survey on various trust computation mechanisms, trust dynamics and their inter operations are missing in [20]. These are all essential components of trust system and seek a cohesive survey given the volume of literature available in these specific areas.

Our contributions: In this paper we attempt to fill the gap in the existing survey literature by providing a focused survey on various trust computing methods and trust dynamics pertaining to MANET. We consider trust propagation, aggregation and prediction as the main trust dynamics which can help in trust computations. Our proposed MANET trust system contains the following functional blocks as shown in Fig. 1:

- Trust computations based on metrics and definitions
- Trust propagation
- Trust aggregation
- Trust prediction
- Trust applications

First of all trust value of the node will be computed (trust computations) based on some metrics or recommendations. This trust computation can be centralized or distributed as shown in Trust computations block of Fig 1. These computed trust values will be propagated in the network so that the trust can be

established between nodes which are not in immediate contact. While propagating the trust, trust values from multiple paths will be aggregated to get a combined trust value which can be stored in the history. The stored trust value will be used in the trust predictions and this predicted trust value will be further used in the applications that need security. The stored trust value can also be used in the trust computation block in the form of feedback knowledge. Therefore, trust computations, trust propagation, trust aggregation and trust prediction blocks are closely interconnected in our envisioned trust system.

We organize this survey by keeping the envisioned model in Fig 1 as reference. Section II discusses definitions, metrics and properties that are used to compute trust in various existing literature. Section III gives detailed summarization of different approaches available on computing trust. Section IV provides summary of the literature available on various trust dynamics. Survey of various literature on the application of trust in security is provided in Section V. Future research opportunities on trust and concluding remarks are given in Section VI.

II. Trust Definition, Metrics and Properties

To compute the trust level on nodes, it is important to understand trust definition, metrics and various trust properties that are employed in trust computations.

A. Definition

There are several definitions given to trust in literature. Trust can be reflected by reliability, utility, availability, reputation, risk, confidence, quality of services and other concepts. Nevertheless, none of these concepts can accurately describe the definition of trust. This is because trust is an abstract concept, which combines many complicated factors [21].

Trust has received attention in several literatures: psychology, sociology, economics, political science, anthropology and recently in wireless networks [22], [23]. Each literature approaches the problem with its own disciplinary lens and filters. For example, while sociologists tend to see trust as relationship in nature [24], [25], some psychologists consider it as a personal view/attribute [26]. Social psychologists are more likely to consider trust as an interpersonal phenomenon [27] whereas Economists are more inclined to view trust as a rational choice mechanism to increase its own utility [28].

With respect to MANET sense, these definitions can be classified into following:

1) Trust as risk factor: The definition given by Morton Deutsch [3] is more widely accepted than many, and states that trusting behaviour occurs when an individual (node) perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person. In [29], [30] trust is defined as a bet about the future contingent actions of others.

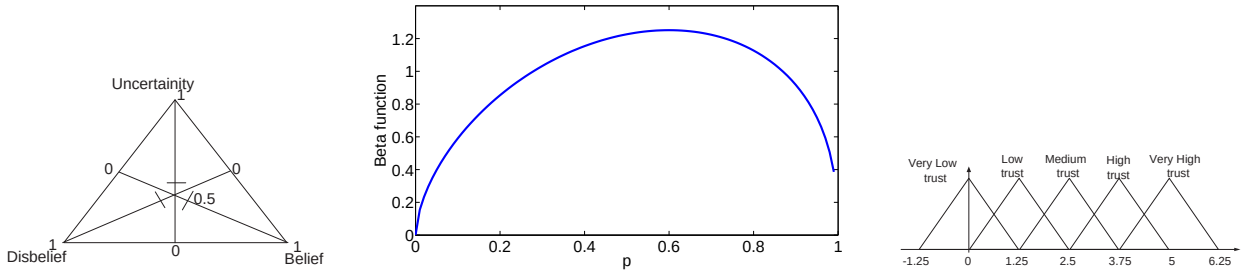
2) Trust as belief: Trust is an individual's belief and willingness to act on the basis of the words, actions, and decisions of another [31]–[37].

3) Trust as subjective probability: Trust (or distrust) is a particular level of subjective probability with which an agent will perform a particular action for a specified period within a specified context [16], [38]–[41].

4) Trust as transitivity relationship: Trust is a weighted binary relation between two members of a network. As an example, consider a network of intelligence gathering agents, organized in a hierarchical manner. Trust could then be seen as the expectation of a person A (presumably high in the hierarchy) that a person B (low in the hierarchy) is honest, as opposed, being a double agent [42].

Summary:

We can summarize the definition of trust in the MANETs perspective in the following way: The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context.



(a) Trust as belief function (b) Probability based trust (c) Fuzzy logic based trust

Figure 2. Pictorial representation of the various metrics used to measure the trust

Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/behaviour. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted by the given node.

B. Metrics

Trust has been evaluated using different metrics and different ways. We can classify the work on trust metrics in the following categories:

1) Trust scale: Some schemes use continuous or discrete values to measure the level of trust. For example, in [43]–[46] trust is described by a continuous value in $[0,\ 1]$ and in [35] trust is measured as discrete value in $[-1,\ 1]$. Threshold based approaches are also used to measure the trust. For instance in [47], if the normalized amount of satisfaction with respect to the number of interactions is greater than some threshold then the node will be considered as trustworthy.

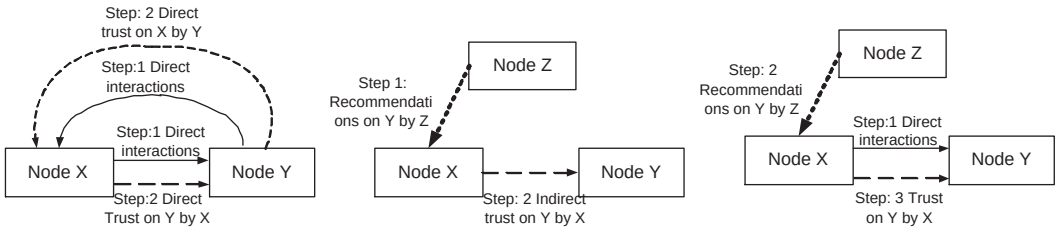
2) Trust facets: In [48], a confidence value c in the interval $[0,\ 1]$ and a trust value in the interval $[0,\ 1]$ together denote the trustworthiness of a node. The trust value (T) represents the observed trust value and confidence value (C) represents the level of confidence a node has on the observed trust value. Now the shortest distance from origin to $(T,\ C)$ on a 2D rectangular plane denotes trustworthiness. In [49], [50], the metric is a triplet (b, d, u) $\in [0,1]^3$ b + d + u = 1, where b, d, and u denote belief, disbelief, and uncertainty respectively. Trust is represented in this triplet space as shown in Fig. 2. a.

3) Trust logics (probability, fuzzy): Some of the approaches use probability as metric for trust. [51], [52] use the probability metrics to determine trust while [53] uses the ratio between number of packets forwarded correctly to the total number of packets received as a trust metric. In [54] Beta distribution is used. Here the bad and good experiences are used in the Beta distribution to obtain the trust value. The Beta distribution plot for various Beta parameter p and fixed good experience factor $\alpha = 1.7$, bad experience factor $\beta = 1.3$ is shown in Fig. 2. b. The mean value of this distribution gives trust value.

Some literature use fuzzy logics to represent trust [35], [55]–[57]. In fuzzy logics, some labels (mainly adjectives) from natural language are used for assigning values; each label represents a range of possible values. For instance in Fig. 2. c trust value of range $[-1.25,\ 1.25]$ denotes very low trust and so on. In Fig. 2. c a node who has 0.25 trust is assumed to have 75% very low trust and 25% low trust [58].

Summary:

After analyzing the various metrics used for trust computations in the literature, we conclude that trust is a relative factor and hence can be represented as a value either confined in the interval $[-1,\ 1]$ *(where*



(a) Neighbour sensing based direct trust establishment

(b) Recommendation based indirect trust establishment

(c) Hybrid method of trust establishment

Figure 3. Pictorial representation of the various computing schemes

the distrust can be represented by -1 *and complete trust can be represented by* 1 *[35]) or through some probabilistic metric.*

C. Trust properties

Next, we deal with properties that are important for trust computations. Based on [59], [60], we consider three main properties of trust that hold in trust networks: Asymmetry, Transitivity and Composability. Asymmetry means, if A trusts B at a certain level, it does not necessarily mean that B trusts A at the same level.

Transitivity property implies that trust can be passed along a path of trusting users. If A trusts B and B trusts C, it can be inferred that A trusts C at a certain level.

Composability means that trust information received from all available paths can be composed together to obtain a single opinion value.

III. TRUST COMPUTATIONS

Trust computations consist of three components: 'experience', 'recommendation' and 'knowledge' [61]. The 'experience' component of trust for each node is directly measured by their immediate neighbours and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as 'recommendation' part of the trust. At a regular interval, the previously evaluated trust is included in the current 'knowledge' component of total trust. Now either these three components individually or a combination of them can be used in computing the trust.

The work on trust computations can be broadly classified into the following categories:

- Distributed trust computations: Every node computes its own value of trust on its neighbours
- Centralized trust computations: Central agent manages/helps the node in trust computations

We explain the research efforts on these subjects in detail in the following sections.

A. Distributed trust computations

Distributed trust computations can be classified as: Neighbour sensing (Direct trust), Recommendations based trust (Indirect trust), and Hybrid method as shown in Fig 3.

Neighbour sensing (Direct trust):

Distributed trust computation based on neighbour sensing is illustrated in Fig 3. a, where every node observes neighbours for their event reports and stores the reports in 'knowledge' cache. A trustor node (trust measuring node) will compare its own observation report on event with the observation report it

received from the trustee node (nodes trust need to be measured) and also from other close by neighbour nodes. Trust factor will be determined based on amount of deviations between the observation reports [62].

A trust establishment strategy based on packet routing and acknowledgement schemes for adhoc networks is proposed in [63]. Trust of a particular node x is calculated by a node y as follows:

$$T = W(R_p) \times R_p + W(R_q) \times R_q + W(R_e) \times R_e + W(D) \times D \tag{1}$$

where $W(.)$ is a weight assigned to a particular event, $R_p,\ R_q,\ R_e,\ D$ are normalized route reply misbehaviour factor, route request misbehaviour factor, route error misbehaviour factor and data delivery misbehaviour factor respectively. The values of $R_p,\ R_q,\ R_e,\ D$ are determined as follows:

$$R_p = \frac{R_{ps} - R_{pf}}{R_{ps} + R_{pf}}, R_q = \frac{R_{qs} - R_{qf}}{R_{qs} + R_{qf}}, R_e = \frac{R_{es} - R_{ef}}{R_{es} + R_{ef}}, D = \frac{D_s - D_f}{D_s + D_f} \tag{2}$$

where R_{ps}, R_{qs}, R_{es} and D_s are the number of successful: route reply acknowledgement packets, route request acknowledgement packets, route error acknowledgement packets and data delivery acknowledgement packets, respectively. Similarly R_{pf}, R_{qf}, R_{ef} and D_f are the number of failed packets.

A trust computation method based on direct observations to establish trust among sensor nodes is proposed in [52]. Every node measures the trust of the other nodes by analyzing their behaviour over time. For instance, x observes the behaviour of y and judges whether the behaviour is correct or not. Each opportunity x has of observing the behaviour of y is recorded in an experience record cache. Over the time, these experiences will become stale. Therefore, x will assign some weight values (decreasing function with time) to the past history. Here trust is represented as mean trust value and a confidence interval about the mean. Authors assume that x_i is the inference by node x on node y's behaviour at time i and the weight factor assigned to this inference is W_i. The mean value of inference over time n is given by

$$\bar{x} = \sum_{i}^{n} \Big(\frac{W_i}{\sum_i^n W_i} x_i \Big) \tag{3}$$

The value of W_i depends on both the behaviour of node y at ith experience as well as the trust value of x in measuring the trust of y. Now the variance around the mean is given by

$$\sigma^2 = \sum \Big(\frac{\sum_i (x_i - \bar{x})^2}{n-1} \Big) \tag{4}$$

The weighted variance is given by

$$\sigma_W^2 = \frac{\sigma^2 \sum W_i^2}{\left(\sum W_i\right)^2} \tag{5}$$

This weighted variance is used to create a confidence interval about the mean as follows

$$\bar{x} \pm t_{n-1,1-\alpha/2} \sqrt{\sigma_W^2 / n} \tag{6}$$

where α is 0.10 for 90% confidence interval, 0.05 for 95% confidence interval, etc. The t in the above equation represents the $student - t$ distribution. If this confidence interval is sufficiently narrow then x will proceed with its decision-making process. However, if the confidence interval is too wide then additional experiences will be collected. Though, this method is proposed for adhoc sensor networks, it is generic enough and can be applied to MANETs as long as the nodes are identified with some unique address.

A distributed trust evaluation based on Bayesian network for MANET is proposed in [64], [65]. A Bayesian network is a relationship network that uses $Beta$ distribution combined with Bayesian estimate to determine the trust relationships among the nodes. $Beta$ distribution is initially employed to determine

the prior trust relationship based on the past interactions. Then likelihood function is used to determine the probability of success. Now, the prior trust level and likelihood functions are used in the Bayesian posterior estimate to determine the final trust of the node.

Recommendation based trust:
Distributed trust computations based on recommendation systems is shown in Fig 3. b. Here, trust relationships on nodes are established based on recommendations alone.

A trust establishment strategy based on local voting for adhoc networks is presented in [66]. A trust network graph G is formed where nodes are connected if they are one hop away in terms of physical transmissions. Now, every node has a trust value either $+1$ or -1 ($+1$ for full trust and -1 for untrust) with the confidence of $c \in [+1,\ -1]$ on every other node. In this voting scheme $c_{ij} = 1$ represents completely positive confidence i has on j, $c_{ij} = -1$ represents completely negative confidence and $c_{ij} = 0$ means totally uncertain, i.e i and j have no interactions. Trust relations are asymmetric, i.e $c_{ij} \neq c_{ji}$. In the voting rule suppose node i is the target of trust evaluation, all the opinion values on i from neighbours will be aggregated to form a trust value. Since the recommender itself may be a misbehaving node, instead of just using summation as aggregation the authors propose an effective voting scheme. The effective confidence value between i and j is given by:

$$\hat{c}_{ij} = \frac{c_{ij} + c_{ji}}{2} \tag{7}$$

Authors assume $s_i(k)$ is the trust value of i at kth instance and the trust value at the $k+1$th instance is given by

$$s_i(k+1) = \begin{cases} 1 & \text{if } m_i(k) > \eta \\ -1 & \text{if } m_i(k) < \eta \end{cases}$$

where η is some threshold and $m_i(k)$ is given by

$$m_i(k) = \sum_{j \in N_i} \hat{c}_{ji} s_j(k) \tag{8}$$

where N_i is the number of nodes in the small network in which every node is connected. Authors also propose a global voting rule where instead of just N_i nodes, the opinion from all the nodes in the network is considered in computing trust.

An extension of the work in [66] is presented in [67]. The evaluation process was modelled as a generalized shortest path problem on a directed trust graph $G(V, E)$, where nodes V represent entities, and strength of edges E represent trust relations (strong or weak). The idea is to combine the trust value and confidence value into a single opinion value from source to destination in a multihop communication.

A trust establishment scheme based on threat reports for MANETs is proposed in [68]. Every node is equipped with an intrusion detection system (IDS). Every node monitors its one hop neighbour nodes and generates "trust report" based on the neighbour nodes behaviour. Initially all nodes will have a random unknown trust level on other nodes. Once the trust report is generated it will be either broadcasted to all nodes or it can be flooded controllably in the network. In case any node generates false report it will be detected by IDSs on neighbouring nodes. The IDS monitoring is capable of noticing large discrepancies in trust reports and should broadcast the information about the false reports to all the nodes.

Hybrid method:

In this method the trust on a node is computed based on direct experience and also recommendations from other nodes as shown in Fig 3. c.

A trust formulation based on linear combination of self evaluated trust ($0 \leq T_s \leq 1$) and other nodes evaluated trust ($0 \leq T_o \leq 1$) for MANETs is proposed in [69]. The node x's trust on node y is given by

$$T_{x,y} = \alpha T_s + \beta T_o \tag{9}$$

where the constants α and β are such that $\alpha + \beta = 1$. T_s is computed by directly monitoring y for total packets dropped by y, packet forwarding delay by y, packets misrouted by y and packets wrongly injected by y. T_o is the collective trust evaluation by all other nodes on y. Authors propose following four different ways to calculate T_o based on all evaluations:

1) Optimistic or Greedy approach: Trust report received from all nodes about y will be weighted by their own trust value. Now, the maximum of weighted trust evaluation is selected as T_o.
2) Simple Average of Weighted Products: Average of weighted trust evaluation by all other nodes on y is selected as T_o.
3) Weighted Average: Weighted average of weighted trust evaluation by all nodes on target node y is selected as T_o.
4) Double Weighted Approach: Here each trust evaluation is divided by sum of all trust evaluations. This factor is used as weighting function in calculating the weighted average of weighted trust evaluation.

An approach similar to Eq. (9) is analyzed in [70]. The trust evaluation of node a about node b ($T_a(b)$) is given by

$$T_a(b) = (1-\alpha)Q_a(b) + \alpha R_a(b),\ 0 \leq \alpha \leq 1,\ 0 \leq Q_a(b) \leq 1,\ 0 \leq R_a(b) \leq 1 \tag{10}$$

where $Q_a(b)$ represents the trust node a has on node b based on its own observations and $R_a(b)$ is the aggregate value of the recommendations from all other neighbors about b. Now

$$Q_a(b) = \beta E_a(b) + (1-\beta)T_a(b),\ 0 \leq \beta \leq 1 \tag{11}$$

where $E_a(b)$ represents the trust value obtained by the judgment of the actions of b and $T_a(b)$ gives the last trust level value stored about node b on node a.

A time-sensitive and context-dependent reputation schemes are proposed in [71] for MANETs. Here the combination of direct trust and recommended trust is termed as reputation. In the case of time-sensitive reputation scheme the recent behaviours are given more weight than the past history. In context-specific reputations, if a particular target context does not generate much data, then the reputations on this target context can be derived from other context which has good amount of data about the target.

In [72] the trust value of node i on node j at time $t+1$ ($T_j^i(t+1)$) is computed as combination of direct trust of i on j at time t ($DT_j^i(t)$) and recommended trust on j to i by some other nodes at time t ($RT_j^i(t)$) as follows

$$T^i(t+1) = \alpha \times DT_j^i(t) + (1-\alpha) \times RT_j^i(t),\ 0 \leq \alpha \leq 1 \tag{12}$$

An information theoretic framework to quantitatively measure the trust for distributed adhoc networks is given in [73] and [74]. A distributed scheme is designed to acquire, maintain and update trust records based on the packet forwarding behaviour of nodes. For illustration, assume that node x wanted to measure the trust level of node y and $p = P(x, y, task)$ is the probability of y performing the "$task$" in the point of view of x. Now, the trust value on y measured by x with respect to "$task$" is given by

$$T(x, y, task) = \begin{cases} 1 - H(p) & \text{if } 0.5 \leq p \leq 1 \\ H(p) - 1 & \text{if } 0 \leq p \leq 0.5 \end{cases}$$

where $H(p) = plog_2(p) - (1-p)log_2(1-p)$.

Trust computation based on evidences collected from other users and also the self evidences is proposed in [75], [76]. Dempster-Shafer theory is used to combine the evidences. In Dempster-Shafer theory *basic probability assignment (bpa)* is used to model the direct interactions between two nodes [77]. The *belief function (Bel)* is used to model the belief factor on the nodes with which a particular node never interacted. *Bel* is formulated based on recommendations. Now, the Dempster-Shafer rule of combination is employed to combine *Bel* and *bpa* to determine the final trust.

A trust representation based on probability-certainty density function (PCDF) is proposed in [78]. PCDF is derived using the probability and certainty notions. An extension of this work is presented in [79]. A mechanism is provided to update the trust values of nodes, based on the behaviours they exhibit. Following the similar procedure in [80] the trust of a node is modelled in two spaces i.e., evidence space and belief space. In evidence space, the trust value of a node y is represented in terms of r, s, where $r \geq 0$ is the number of positive evidences and $s \geq 0$ is the number of negative evidences ($r + s \geq 0$). Now, $\alpha = \frac{r}{r+s}$, is the average trust in evidence space. In the belief space, a trust value is modelled as a triplet $b,\ d,\ u$, where $b,\ d,\ u \geq 0$ and $b+d+u = 1$. A bijective trust transformation is used to transform the trust from evidence space to belief space.

A trust computing framework based on transaction-based feedback for a structured P2P network is proposed in [47]. Authors assume that $I(u)$ denotes the total number of transactions performed by node u with all other peers, $p(u, i)$ denotes the other participating peers in node u's ith transaction, $S(u, i)$ denotes the normalized amount of satisfaction node u receives from $p(u, i)$ in the ith transaction, $Cr(v)$ denotes the credibility of the feedback submitted by v, $TF(u, i)$ denotes the adaptive transaction context factor for node u's ith transaction, and $CF(u)$ denotes the adaptive community context factor for node u. Now the trust value of node u is,

$$T(u) = \alpha \sum_{i=1}^{I(u)} S(u, i)Cr(p(u, i))TF(u, i) + \beta \times CF(u) \tag{13}$$

where α is the normalized weight factor for the collective evaluation and β is the community context factor.

A hybrid trust evaluation scheme using the approach of Trust Overlay Network (TON) for P2P network is proposed in [81]. In the TON local trust scores between peers are represented as connection strength in the graph. The number of feedbacks an user sent to others is indicated by the out-degree of the peer node. The number of feedbacks an user received from others is represented as the in-degree of a peer node. Now the global reputation values are chosen from the local trust value of ToN using random Markov walk.

A reputation scheme using distributed polling for P2P networks is proposed in [82]. In this approach resource requesters assess the reliability of a resource offered by a participant using the distributed polling. This P2P trust model works on the basis of both direct 'experience' and also 'recommendation' from other peers.

A detailed comparison of different distributed trust computing schemes with respect to context in use, advantages, complexity and performance limitations is provided in Table I.

The absence of fixed trust infrastructure, limited resources, ephemeral connectivity, shared wireless medium and physical vulnerability make distributed trust establishment challenging. To overcome these problems, some of the literature propose trust establishment in adhoc networks using a number of assumptions including the presence of an omnipresent central trust authority or trust agent. In the following section we review some of the trust establishment schemes based on trust agents.

B. Centralized trust establishment

Most of the work on the centralized trust establishment assumes a Trust Agent (TA) which can be accessible by all nodes in the group as shown in Fig. 4. Here the TA either computes the trust for the whole community or assist the nodes in their trust computations by providing the initial trust values on target nodes. There could be one or many TAs based on the size of the network.

A centralized cluster head based trust computation is proposed in [84]. Every node in the cluster first obtains the initial trust value on every other node from the cluster head. Now a node will combine its

Table I
COMPARISON OF DIFFERENT DISTRIBUTED TRUST COMPUTING MECHANISMS

Authors and Year	Context in use	Trust and performance metrics	Advantages	Complexity	Performance and limitations
Direct trust computations					
M. J. Probst et. al, 2007 [52]	Based on observing the neighbours behaviour over the time.	Trust is a fractional value in $[0, 1]$. Convergence time, memory cache requirements are analyzed.	Accumulates the past behaviours and weigh them based on time. Hence the trust computation is precise. No single point failure.	Requires memory to store the past experiments. Computational complexity to determine the t-distributions.	Trust computation is completely local and biased.
A. A. Pirzada et. al, 2006 [63]	Routing based direct trust calculations.	Trust is a fractional value in $[0, 1]$. Performance of AODV and DSR protocol have been analyzed with the proposed trust scheme.	Works based on existing request and acknowledgement schemes in AODV and OLSR protocols. This local trust is precise [41]. No single point failure.	Additional hardware to monitor the packet drop/forward event of neighbours.	Specific to routing. Nodes should monitor neighbours all the time to construct and update trust relations. Computed trust is biased.
S. Buchegger et. al, 2004 [64], C. Zouridaki et. al, 2005 [65]	Past actions and present behaviour are combined in Bayesian estimate to determine trust.	Trust is measured as probability value. The improvement of trust for various numbers of observations has been analyzed.	No single point failure.	Observation collection and Bayesian calculations requires memory and computational complexity.	Measurement is totally instantaneous and may not be precise.
Recommendation based trust					
T. Jiang, 2006 [66] G. Theodorakopoulos, 2006 [67]	Based on local voting.	Trust is measured in $[-1, 1]$. Bad nodes recognition rate is used as performance metric.	Combines the trust measurement with the confidence value using semiring principle. Hence the trust is represented in a precise way.	Extra memory to store the recommendations. Computational complexity in semiring combining.	It does not consider the historical behaviour of nodes.
Z. Liu et. al, 2004 [68]	Trust evaluation based on controlled flooding recommendations.	Trust is measured in $[0, 1]$.	No additional hardware or computations required.	Flooding will create communication over heads.	The convergence time in trust computations and readjustments are high.
Hybrid trust					
L. Xiong et. al, 2004 [47]	Based on feedback recommendation and own evaluations in P2P network.	Trust is measured in $[0, 1]$. Transaction success rate and malicious node detection rate are used as performance metrics.	Feedbacks are weighted based on credibility factors and also community context is taken into account. This can provide accurate results.	Communication over head in collecting the feedback recommendations.	The feedback can be represented only in binaries 0 or 1. Hence the feedback recommendations may not be accurate.
P. B. Velloso et. al, 2010 [70]	Based on recommendation aggregation and also neighbour sensing.	Trust is measured in [0, 1]. Trust convergence and asymptotic error behaviour are analyzed.	The recommendation aggregations and combining the recommendations with self measurement can increase the trust accuracy.	Memory requirement to store the past value.	This approach will be ineffective in spare networks.
Y. L Sun et. al, 2006 [73], [74]	Measurement based on packet forwarding behaviour.	Trust is measured as entropy in $[0, 1]$. Adaptive change in trust value for various number of compromised nodes has been anaylsed.	Trust calculation is based on actions and task. Hence this approach is generic enough and can be applied in any networks.	Additional hardware to sense the neighbours. Computational complexity in calculating the entropy and trust.	It does not use either recommendations or the past observations. Hence the trust measurement is totally instantaneous and node dependent.
B. Yu et. al, 2002 [75] and N. Wilson et. al 2000 [77]	Works based on both direct interactions and also evidences collected.	Trust is represented as belief function which is a probability measure. Trust convergence has been analyzed in detail.	This approach is generic enough to be used in all situations where the evidences are independent. No single point of failure.	Computational complexity of belief function generation and also Dempster-Shafer theory of evidence combining.	Dempster-Shafer theory can work only for combining independent evidences [83].

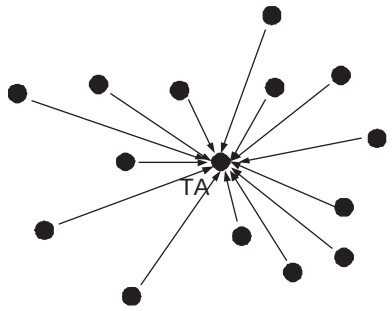


Figure 4. Pictorial representation of the TA based centralized trust computation methods

own calculated trust value on neighbour based on experience with the initial trust value obtained from the cluster head. For instance, node i evaluates the trust of node j ($\phi(i,j)$) as follows:

$$\phi(i,j) = T(i,j) \times \alpha + T(H,j) \times (1-\alpha) \times \beta \tag{14}$$

where $T(i,j)$ is the trust value calculated by node i on j based on successful data delivery rate and successful experience rate, $T(H,j)$ is the initial trust value obtained from cluster head on node j and β is malicious factor ($\beta = 0$ denotes malicious and $\beta = 1$ denotes non-malicious). Now all nodes will report their trust evaluation by all nodes on the target node to cluster head. Cluster head will multiply each evaluation value with the trust value of the provider and then average them all to determine the final trust value. This trust value will be distributed to all the nodes as trust certificate.

An agent-based trust and reputation management scheme for MANET is proposed in [85], [86]. Authors assume n number of reputation assistants. A node C who wants to evaluate the trust of the neighboring node x will query its reputation assistants about this neighboring node x. After receiving the trust values from its reputation assistants, C uses the weighted means to measure the nodes final trust and then makes the corresponding decision. The following formulae are used to determine the final trust of C on X (T)

$$Trust_{AVG} = \frac{\sum_{i=1}^{n} Trust_{RA_i,X}}{n} \tag{15}$$

$$w_i = \frac{Trust_{RA_i,X}}{Trust_{AVG}} \tag{16}$$

$$T = \frac{Trust_{C,X} + \sum_{i=1}^{n} w_i \times Trust_{RA_i,X}}{n+1} \tag{17}$$

where $Trust_{AVG}$ is the average agent (reputation assistant) trust on X, $Trust_{RA_i,X}$ is the trust of reputation assistant i on X, w_i is the weight given to trust value obtained from assistant i and $Trust_{C,X}$ is the self measured trust of node C on X.

A trust modelling scheme for a group of nodes (group trust) based on cluster head approach is proposed in [87]. The entire network is divided into number of small groups and every group has a cluster head and all the cluster heads are connected to the base station. Inside the group, distributed trust management approach is used. For instance, inside a group node x calculates the trust on node y based on both direct interaction ($PI_{x,y}$) and peer recommendation ($PR_{x,y}$). The direct trust ($PI_{x,y}$) is evaluated by storing the past actions. The recommended trust on y is calculated as follows:

$$PR_{x,y} = \frac{\sum_{i=1}^{n-1} \left[TV_{x,i} \times TV_{i,y} \right]}{n-1} \tag{18}$$

Table II
COMPARISON OF DIFFERENT CENTRALIZED TRUST COMPUTING MECHANISMS

Authors and year	Context in use	Trust and performance metrics	Advantages	Complexity	Performance and limitations
S. S. Park et. al 2008 [84]	Clustering based trust computations.	Trust is measured in the interval $[0,\ 1]$ using Beta distribution.	The computed trust is global and not biased.	Complexity in maintaining the cluster and electing the cluster heads.	The computed trust may not be precise with respect to single particular node. Cluster head can be single point of failure.
A. Boukerche et. al 2008 [85], Y. Ren et. al 2008 [86]	Nodes query the agents for the initial trust and then calculates the final trust value based on averaging.	Trust is defined in the interval $[0,\ 1]$. Malicious node handling, security over head and community sizes have been analyzed.	This scheme can handle collusion attack well as the trust is bootstrapped from the reputation agent.	Infrastructural complexity of maintaining more than one trust agents and the reliable communications from the agents to the nodes.	This scheme will perform well as long as number of reputation agents are high.
R. A. Shaikh et. al 2006 [87]	Cluster head aggregates the trust reports received from individual nodes and determines the final trust.	Trust is presented as fuzzy logic in the intervals $\{0-0.4, 0.4-0.6, 0.6-1\}$. Memory requirements have been analyzed.	Global trust value.	Complexity of maintaining high trustworthy communication between cluster heads and cluster heads to base station.	Cluster head can be single point of failure.
B. Lagesse et. al 2009 [88]	Based on a centralized *Trust Block* which collects votes and calculates the trust.	Trust is confined in the range $[0,\ 1]$. The impact on trust computations by increasing the peer numbers has been analyzed.	This trust algorithm can be made adaptive by changing the *presentation unit* of the *Trust Block*.	Infrastructural and computational cost of hosting *Trust Block*.	*Trust Block* could be single point of failure.

where $TV_{x,i}$ is the trust value of node i calculated by node x and $TV_{i,y}$ is the trust value on node y sent by node i and n is the total number of nodes in the group. The final trust value on y by x is the average of $PI_{x,y}$ and $PR_{x,y}$. This trust value will be sent to cluster head. The cluster head will determine the trust value of other cluster heads based on interactions and then forward all the information to the base station. Base station will then decide the trust factors (fully trust, untrust or uncertain).

Trust evaluations for pervasive systems using a framework called Distributed Trust Toolkit (DTT) is presented in [88]. DTT has two abstractions namely: Trust Blocks and Trust Groups. Trust Block contains everything needed to compute the trust of a node. Trust Block has three modular components to compute the trust: *Computing*, *Presentation* and *Protocol*. The *computing* component is responsible for implementing the algorithms involved in computing the trust values. The *presentation* component makes policy decisions based on data gathered by the *computing* component. The *protocol* component implements network-based trust protocols and allows the DTT to inter operate with legacy trust systems. Trust groups are formed between nodes on the basis of both mutual trust and the expectation that they will benefit by joining the group. In this dynamic group a strong and powerful node in terms of computation and power backup will be elected to host the Trust block.

Comparison of different centralized trust computing schemes with respect to context in use, advantages, complexity and performance limitations is provided in Table II.

C. Attack model

Trust computations and management can be attractive target for attackers since major decisions can be taken based on the trust computations. In this section we identify some possible attacks for the trust

schemes in MANETs and then compare trust computing schemes based on these attacks.

1) Denial of service attack (DOS): In the DOS attack the attackers send as much trust recommendations as possible to consume the large amount of computing resources in the trust calculating nodes [89]. DOS attack can be successfully handled in neighbour sensing trust computing method as it does not depend on the trust reports. However, the rest of the trust computing methods can be affected by DOS attack.

2) Bad mouthing attack (BMA): Bad mouthing attack occurs when a node gives bad recommendation intentionally about other nodes. This attack is very common in recommendation based trust computing methods [90]. All other trust computing methods can handle BMA well because mostly they are based on the aggregations of multiple observations [12].

3) On-off attack (OOA): In this type of attacks malicious entities can opportunistically behave good and bad as per the importance of situation [91]. To handle the OOA the observation made long time ago should not carry the same weight as that of recent one [92]. In the case of neighbour sensing, mostly the recent samples are taken into account for trust calculations [52]. In all the remaining methods the observations made by many sources are collected and aggregated together. As long as the on period (active attack period) is larger than off period and also the number of attackers are less, at least few of the observing node can pick up the bad behaviour of the node [92]. Therefore, OOA attack can be successfully handled by all the trust computing methods.

4) Conflicting behaviour attack (CBA): In this attack, malicious entities behave differently towards different nodes. For example, it can give a good recommendation about particular node to one group of nodes and bad recommendation about the same node to other set of nodes. These conflicting recommendations can confuse the trust evaluation system and eventually degrade the performance. For the same reasons as that of OOA, CBA also can be handled by all the trust computing methods.

5) Sybil attack (SA): In Sybil attack a malicious node will create several fake IDs. These fake IDs can share or even take the blame, which should be given to the actual malicious node [93], [94]. In [95] it is shown that without the centralized authority it is always possible to launch the SA. Even in the case of centralized systems when the Sybil identities are large in number, the aggregation operation may rule the attacker as genuine node [96]. Multiagent based trust computations can handle the SA as the collaborations among various agents can detect the fake identities [97]. However, the cost paid is the infrastructural complexity.

6) Camouflage attack (CA): In camouflage attack, the dishonest users attempt to build up trust by always reporting as per the observed majority. After they earn enough trust values, they behave dishonestly only for specific occasions. CA can be detected as long as the number of bad behaviours is significantly large and the bad behaviours are given high penalty [92], [98]. However, when the number of bad behaviours are less both neighbour sensing and recommendation based schemes can be affected by this attack as the attackers can easily get away with good trust scores. Centralized trust schemes can detect these behaviours since in these schemes there are large number of observers observing the target node.

7) Collusion attack (CoA): Collusion attacks are engendered by more than one malicious node collaborating and giving false recommendations about normal nodes through the recommendation parameters. Neighbour sensing works based on direct observation of each node. Hence, it is not prone to collusion attacks [99] and also the hybrid approach [81]. However, all other trust computing methods can suffer significantly by CoA.

8) Newcomer attacks (NCA): In this attack, the attacker simply leaves the system and joins again hoping to flush out the previous bad history and to accumulate new trust [100]. Recommendation based systems and centralized trust computing system can handle NCA well as some of the neighbour node of the malicious attacker can detect this behaviour and report it. However, neighbour sensing based on present action, can suffer considerably by this attack.

These are all widely discussed and generic attack models for the trust computations. Apart from these, some application specific attack models are discussed in [20], [101], [102].

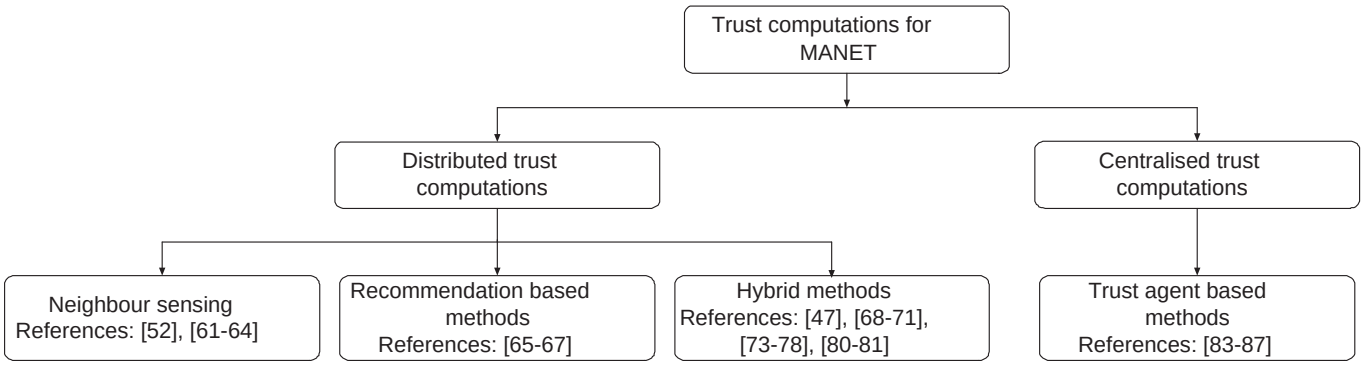


Figure 5. Trust computing methods classifications

Table III
COMPARISON OF DIFFERENT TRUST COMPUTING MECHANISMS WITH RESPECT TO VARIOUS ATTACK MODELS

Trust Schemes	Different Attacks							
	DOS	BMA	OOA	CBA	SA	CA	CoA	NCA
Distributed trust computations								
Neighbour sensing	✓	✓	✓	✓	×	×	✓	×
Recommendation based methods	×	×	✓	✓	×	×	×	✓
Hybrid methods	×	✓	✓	✓	×	✓	✓	✓
Centralized trust computations								
Trust agent based method	×	✓	✓	✓	×	✓	×	✓

Summary:
Trust computation methods can be chosen based on the deployment region, applications, level of infrastructure available and the level of precision required. While distributed computations are precise and do not suffer from single point of failure, they are not global in nature and are biased. On the other hand centralized trust computations are global but suffer from single point of failure. The detailed comparison of various trust computations methods under the categories of distributed and centralized trust computations are given in Table I and Table II respectively. Classifications of different trust computing schemes and also the corresponding references used in this paper are given in Fig 5. A broader level comparison of these two categories of trust computing methods with respect to the attack model is provided in Table III where ✓ denotes successful handling and × denotes unsuccessful handling.

IV. DYNAMICS OF TRUST

The evolution of trust over time is called the dynamics of trust. Trust is a dynamic phenomenon. Trust changes with time, experience, and the state of different sources it is based on (e.g., environment, mobility etc). The trust dynamics can be characterized by the following phenomena: trust propagation, prediction and aggregation. In the following we survey the research contributions in these three major trust dynamics.

A. Trust propagation:

Once the trust is computed on target by any of the nodes, the resources spent on recomputation of trust by other nodes can be reduced if the computed trust gets propagated in the network. For instance, in Fig 6 if node A gets to know the trust value of node X through node $B,\ C$, then node A can actually

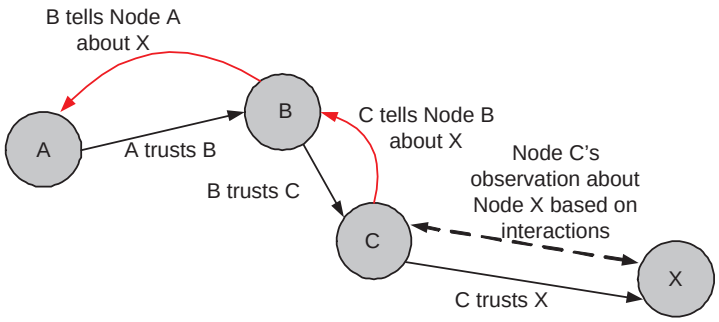


Figure 6. Propagation of trust in a simple straight chain

avoid the explicit trust computation on node X. This is particularly important in MANETs, which feature lack of infrastructure, autonomy, mobility and resource scarcity. Recommendation is the simplest case of trust propagation. Mostly recommendation is from an immediate direct neighbour. On the other hand, trust propagation can be of multi hop. Trust propagation is based on the transitivity property of trust. The core factor to be considered for trust propagation is cooperation in the network in transporting the trust information. If not every node, at least majority of the nodes should cooperate in transporting the trust information.

A trust propagation approach based on the concept of web of trust for mobile networks is proposed in [103] where a web of trusted nodes give rating about the unknown nodes. Based upon this web of trust opinion values, individuals can determine the trust of other individuals (in technical parlance, they propagate trust to other individuals) from whom they have never received content before. Individuals then decide whether to accept the content or not, according to these opinions. The key idea is that each mobile device stores a very limited subset of the web of trust. On that subset, it then applies a machine learning technique for propagating the trust.

Trust propagation in mobile wireless networks using small world concept is proposed in [104]. Here, the trust value is propagated by a transitive graph and this graph confines to the small world phenomenon. Therefore, a node can usually find an authenticating node within few hops. Trust value of this node will be computed by the nodes along the path to the authenticating node. Trust propagation based on transitivity graph is also proposed in [105].

Propagation of trust using the social neighbourhood is proposed in [106]. Here a node a assumed to propagate the trust on node b to all its one-hop neighbours (assume set S) at the same level of trust. That is, trust is assumed to propagate at the same level to all one-hop neighbours. Now all the one-hop neighbours of set S are assumed to get trust level on node b which is degraded by a factor d. This trend continues until the trust level goes below than a threshold.

A trust propagation approach in a highly mobile overlay network using Distributed Hash Table (DHT) is considered in [107]. In order to retrieve information in the distributed and mobile network, DHTs use concepts called Chord, Pastry to store the trust information. These DHTs will hash the network structure into a simple and self-adaptive logical structure. It propagates the trust information into the network, and the retrieve step is bounded by log(N), where N is the number of nodes. This work uses original evidence as trust information, and propagates them under the rule of hash tables.

Propagation of the security credentials and trust information by using mobility is analyzed in [108]. There are certain policies considered: e.g., Friend nodes can carry the trust information and forward them as an authority device. When users meet, they are naturally given the possibility to visually identify each other. The decision to set up a security association between two nodes is based on this physical encounter. To support the mechanism of security association and trust information transition between physically close

Table IV
COMPARISON OF DIFFERENT TRUST PROPAGATION APPROACHES

Authors and year	Context in use	Trust and Performance Metrics	Advantages	Complexity	Performance and limitations
D. Quercia et. al 2007 [103]	Trust propagation and computations using machine learning and web of trust.	Trust is measured in terms of user ratings. Performance of this approach is analyzed in terms of communication, storage and computational overheads.	It uses simple logic for the trust propagation where the propagated trust is weighed with the trust rating of users.	Graph theoretic approach may become complex in large size network.	This approach will not work when malicious node alters their ratings.
E. Gray et. al 2003 [104]	Trust propagation using small world network.	Not applicable. No analysis done.	Simple approach. Trust is propagated through mutually known acquaintance.	No additional complexity.	Cannot work when one of the mutual acquaintance misbehaves in the shortest path of small world network.
S. Trifunovic et. al 2010 [106]	Trust propagation using social neighbours.	Trust is measured in $[0, 1]$. Degradation of trust along the path as the hop length increases is used as performance metric.	Natural way of trust propagation. No extra mechanism required.	No additional complexity.	Trust is assumed to degrade automatically as the hop length increases. This may not be true always.
D. Ingram 2005 [107]	Trust information are exchanged through overlay network using Distributed hash table.	Trust is stored and distributed in the form of evidences. Performance has been analyzed in the presence of collusion attack.	Scalable and attack resistance model.	Complexity in building and maintaining the hash table at each node.	Hash table maintenance and distribution will introduce extra communication and storage over head.
S. Capkun et. al 2003 [108]	Personal meetings are used for trust information exchange.	Trust is propagated in the form of evidences. Dissemination of security services and its convergence time for various mobility models are analyzed.	This approach has minimum over head as the information are exchanged through secure short range channel.	Cost associated with establishing secure channel, key generation and management are very high.	Performance of this approach depends on the mobility patterns and density of the node.
N. Cheng et. al 2011 [109]	Rendezvous based trust propagation.	Probability of malicious node detection is considered as performance metric.	Uses natural mobility of nodes. Less over head compared to flooding based methods.	Minimal complexity.	Trust convergence time is higher compared to flooding based approach.

by nodes, authors assume that each device is equipped with a secure short range connectivity system (e.g., infra-red or wire). In this system mobility can influence the propagation of security and trust information because mobile nodes have more opportunity to interact with many new nodes than static nodes [74].

A rendezvous based trust propagation scheme for MANET is proposed in [109]. Trust requester and trust provider send out trust-request and computed-trust tickets respectively, which will meet in some common rendezvous node with certain probability. The probability of node meeting in common point is analyzed using birthday paradox. The computed-trust will then be propagated to the requester along the trustworthy path.

Comparison of different trust propagation schemes in MANETs is provided in Table IV.

B. Aggregation

When the trust value on a particular target node propagated through multiple paths, multiple versions of this are received at the destination. Now the aggregation operation at the destination can combine these values together to obtain a single trust value. Trust aggregation is based on the composability property of trust. The chain of nodes that transmits the trust information about target node to the trust requesting node constitutes a trust path. The malicious behaviour of one or more nodes on the trust path can alter the trust

information received at the destination. However, when the destination node receives trust value through multiple paths, if one path (e.g. the shortest) yields an unacceptably low level of trust, and other parallel paths yield better trust values, then they can be chosen based on the aggregation operations used. Hence, the aggregation can play important role in suppressing some of the malicious activities. The important factor to be considered for aggregation is the computational complexity. The nodes should be capable of executing the aggregation operations.

In mathematical sense, trust aggregation problem consists of aggregating n-tuples of observed trust values, all belonging to a given set $(x_1, x_2, \ldots, x_n)$, into a single value of the same set (y) as follows:

$$y = Aggre(x_1, x_2, \ldots, x_n) \tag{19}$$

Operators:
Assume that, there are n nodes inferring trust about a particular node and report the trust value $[0,\ 1]^n$ to a trustor node. The aggregated trust using operator $\oplus$ should lie in $[0,\ 1]$. Now, the important conditions for aggregation operator $\oplus$ are [110]
1. Boundary condition:

$$Aggre(0, 0, \ldots, 0) = 0,\ \ Aggre(1, 1, \ldots, 1) = 1 \tag{20}$$

2. Non decreasing conditions
If $y_i > x_i\ \forall\ i$

$$Aggre(x_1, x_2, \ldots, y_i, \ldots, x_n) > Aggre(x_1, x_2, \ldots, x_n) \tag{21}$$

Based on these conditions some basic operators like arithmetic mean, weighted mean and min-max functions can be used as trust aggregation operators [110], [111].

Trust aggregation using subjective logic is proposed in [112]. The authors assume that $E = (r, s)|r > 0, s > 0$ is the observed trust in evidence space, $\hat{B} = (b, d, u)|b > 0, d > 0, u > 0, b + d + u = 1$ is a trust in belief space and $Z(r, s)$ is a transformation from E to $\hat{B}$ such that $Z(r, s) = \Big((B(r, s), D(r, s), U(r, s)\Big)$ where

$$B(r, s) = \alpha\frac{r + 1}{r + s + 2},\ \ D(r, s) = \alpha\frac{s + 1}{r + s + 2},\ \ U(r, s) = 1 - \alpha \tag{22}$$

Let us assume node 1 observes $E_1(r_1, s_1)$ about some node x and node 2 observes $E_2(r_2, s_2)$ about the same node x and $Z_1 = (b_1, d_1, u_1)$ and $Z_2 = (b_2, d_2, u_2)$ are transformations from E_1 and E_2 to belief space respectively. $Z_1 \oplus Z_2 = Z = (b, d, u)$ is aggregated trust in $\hat{B}$ space, where $b = B(r_1 + r_2, s_1 + s_2)$, $d = B(r_1 + r_2, s_1 + s_2)$, $u = B(r_1 + r_2, s_1 + s_2)$. The inverse transform from $\hat{B}$ to E can give the real trust value. Similar aggregation approach is followed in [113].

Iterated belief revision operator [114] is used in [115] to aggregate the trust received from many agents. The node a has some belief about some node x. Now, a receives recommendation about x from the trust agents/other peer nodes. Based on these recommendations node a revises the belief on x. Two aggregation criterion have been considered: (max, max, α) this criteria maximizes the trust upon the maximally trusted node in the resulting aggregation and $(min, mean, \beta)$ minimizes the mean of the differences in trust on the nodes before and after the aggregation.

A gossip based trust aggregation with the gossip average function Push-Sum as an aggregation operator is proposed in [116]. Push-sum is a weighted average aggregation operator derived in [117]. A rumour (trust value about particular node) starts from one node. A node that knows the rumour spreads it to another node chosen uniformly at random. This way rumour can reach all nodes quickly. Once the trustor node receives rumours from many sources, Push-sum operator will be applied to aggregate the rumour values.

Trust aggregation using probabilistic approach is proposed in [118]. Two aggregation schemes have been proposed as shown in Fig 7: sequence aggregation and parallel aggregation. Sequence aggregation aggregates trust along an information flow path. Here conditional independency is assumed, which

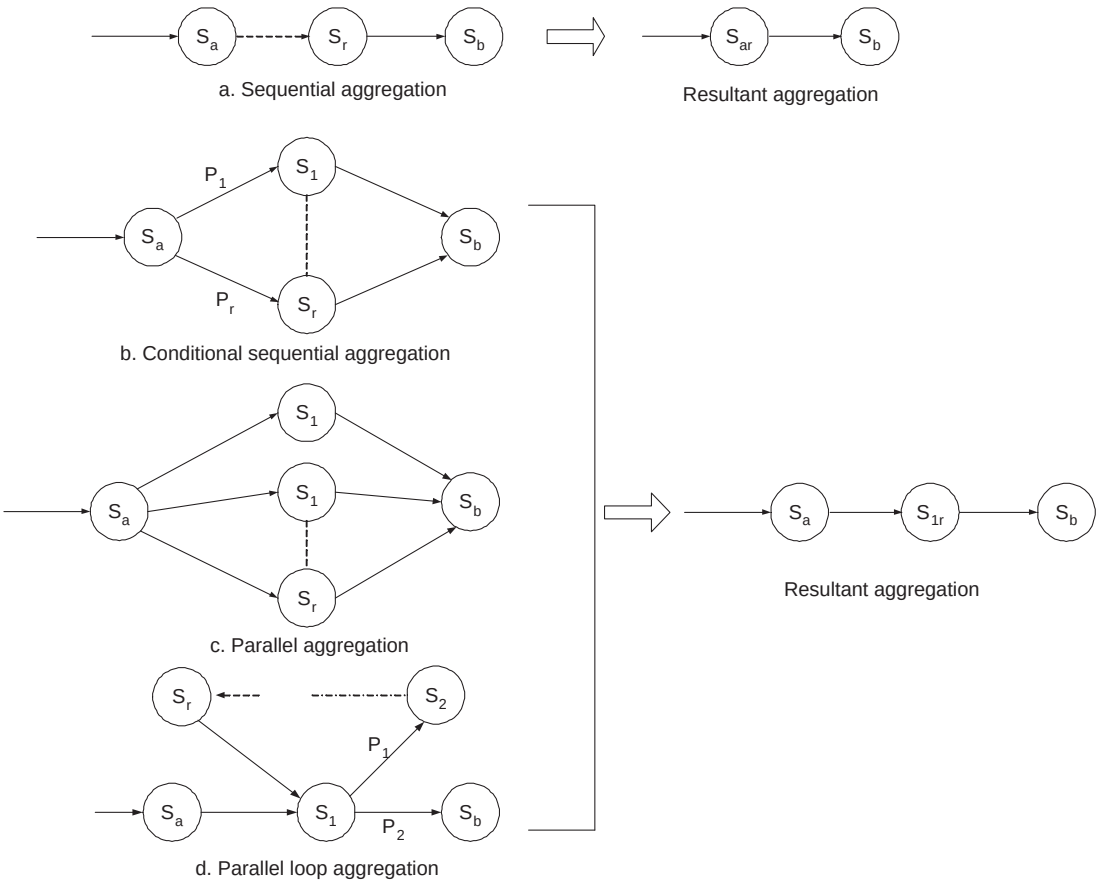


Figure 7. Pictorial representation of various trust aggregation schemes

assumes that an event is directly dependent only on its parents. Parallel aggregation aggregates trust from different parallel paths using different weights. The weight of a path is the ratio between number of samples in that particular path and the total number of samples received.

The Weighted Ordered Weighted Averaging (WOWA) operator is used as an aggregation operator in [119] to compute the aggregated trust. WOWA combines the advantages of both the Ordered Weighted Average (OWA) operator and the weighted mean. WOWA uses two sets of weights: p set of weights corresponding to the relevance of the sources (provenance) and w set of weights corresponding to the relevance of the values.

Several aggregation schemes such as sequence, conditional sequence, parallel and parallel-loop have been proposed in [120]. Here $S_i :: \tau_i$ denotes assignment of trust value τ_i to node S_i, $\&$ denotes AND operator and $\otimes$ is a sequence operator. Now the sequence aggregation of Fig 7. a works as follows

$$S_{12} = \frac{S_1 :: \tau_1 \& S_2 :: \tau_2}{(S_1 \otimes S_2) :: (\tau_1 \otimes \tau_2)} \tag{23}$$

Conditional sequence aggregation is shown in Fig 7. b. The mathematical form of this operation is

$$S_{1r} = \frac{S_1 :: \tau_1 \& S_2 :: \tau_2 \ldots S_n :: \tau_n}{(S_1 \oplus S_2 \oplus \ldots S_n) :: f_{\oplus}(\tau_1, \ldots, \tau_r)} \tag{24}$$

where $f_{\oplus}(\tau_1, \ldots, \tau_r) = \sum_{i=1}^{r} P_i \times \tau_i$, $\sum_{i=1}^{r} P_i = 1$ and P_i is probability of choosing path i.

Table V
COMPARISON OF DIFFERENT TRUST AGGREGATION APPROACHES

Author and year	Context in use	Trust and Performance metrics	Advantages	Complexity	Performance and limitations
Y. Wang et. al 2006 [112]	Subjective logic based trust aggregation.	Trust is represented as triplet in belief space. Set of theorems have been provided to prove various properties.	Trust is aggregated along with uncertainty. Hence the aggregated value is more reliable.	Additional hardware to implement the transformation between trust and belief spaces.	In the belief space every recommendation is given equal weight. Hence it is prone to attacks.
P. Padro, 2009 [115]	Aggregation of trust values using iterated belief and trust revision.	Trust is represented in $[0, 1]$. Aggregation operations are illustrated with examples.	The feedback revision of trust using max and median criterion is a effective method.	Complexity associated with Belief and trust revision.	This aggregation can be used well in the belief based trust system. The only limitation is associated complexity.
Y. Bachrach et. al 2009 [116], D. Kempe et. al 2003 [117]	Weighted average combining of different trust values.	Trust is represented in $[0, 1]$. Set of propositions have been provided to explain the various properties of aggregation operators.	The trust accumulated from different paths are given different weights and hence the chances for attacks are less.	Additional hardware to implement the push-sum and weighted averaging operations.	Less communication load as the gossips are aggregated into single value before retransmission.
J. Huang et. al 2009 [118]	Sequence and parallel aggregation operators are proposed.	Subjective logic is used to represent trust. Various aggregation operators are illustrated with examples.	Along with the trust certainty is also aggregated. This can increase the confidence on the aggregation result.	Additional hardware in terms of multiplications and weighted average.	This work proves that trust propagation through the shortest path may not be highly certain.

Parallel aggregation is shown in Fig 7. c. Parallel aggregation operation among nodes $1, \ldots, r$ is given by

$$S_{1r} = \frac{S_1 :: \tau_1 \& S_2 :: \tau_2 \ldots S_n :: \tau_n}{(S_1 || S_2 || \ldots S_r) :: f_{||}(\tau_1, \ldots, \tau_r)} \tag{25}$$

where $f_{||}(\tau_1, \ldots, \tau_r) = n \sum_{i=1}^{r} \frac{1}{\tau_i}$. Parallel loop aggregation is shown in Fig 7. d. Here the resultant parallel loop operation among nodes 1 to r is given by

$$S_{1r} = \frac{S_1 :: \tau_1 \& S_2 :: \tau_2 \ldots S_n :: \tau_n}{(S_1 \approx S_2 \approx \ldots S_r) :: f_{\approx}(\tau_1, \ldots, \tau_r)} \tag{26}$$

where $f_{\approx}(\tau_1, \ldots, \tau_r) = \frac{P_2 \times \tau_1}{1 - P_1 \times \prod_{1 < i \leq n} \tau_i}$ for $P_1 + P_2 = 1$.

An aggregation operation in the form of multiplication is proposed in [121]. Here the trust values along the path from source to destination get multiplied.
A detailed comparison of different trust aggregation schemes used in MANET is provided in Table V.

C. Trust prediction

Trust prediction is a method of predicting potentially unknown trust between nodes using the present and past behaviour of nodes and also the recommendations received from other nodes.

A pervasive trust model inspired by human system is proposed in [122]. This work uses a set of present observations (i.e., direct experiences) in Kalman filter theory to predict the future state of the system. In this trust prediction model, new trust observations are fed in by means of a set of recursive mathematical equations to increase the accuracy of the prediction. It calculates the discrepancy between the trust value claimed by the node and the actual trust value. Based on this discrepancy the trust of the node will be predicted. Larger is the discrepancy, lower will be the trust value. Another reputation prediction model

Table VI
COMPARISON OF DIFFERENT TRUST PREDICTION APPROACHES

Authors and year	Context in use	Trust and Performance metric	Advantages	Complexity	Performance and limitations
L. Capra et. al 2006 [122]	Uses Kalman filter theory to predict the future trust values.	Trust is measured in $[0, 1]$. Prediction accuracy for various noise covariance matrix is analyzed.	Well established Kalman filter is used for prediction. The prediction accuracy is higher.	Additional hardware complexity in implementing the feedback loop in Kalman filters.	This algorithm can be readily implemented with the expense of additional complexity as Kalman filter is a widely used prediction model.
X. Wang et. al 2010 [123]	Kalman filter based aggregation and prediction.	Trust/reputation is assumed to be a continuous variable bounded in an interval. Convergence time and prediction accuracies are analyzed.	Prediction is based on several observations from many agents. Hence the accuracy is high.	Additional computational complexity in implementing the Kalman filter.	This system may not give good result when the correlation coefficient is less between different observed samples.
C. M. Jonker et. al 1999 [126]	Past actions are used to predict the future trust value using mathematical inductions.	Trust is represented in fuzzy type of descriptions. The update function has been analyzed with quantitative illustrations.	Good accuracy can be achieved as long as more samples are available.	Requires additional memory to store past history of actions. Mathematical induction requires computational resources.	Performance of this system depends on depth of the memory and number of data samples collected.
F. M. Ham et. al 2009 [127]	Internal parameters of the target node is used in trust prediction.	Trust is measured in $[0, 1]$. The convergence time and also false alarms are used as performance metrics.	Generic approach and not depend on applications.	RBF-NN is complex to implement and requires large amount of observations.	The observation of internal parameters of the target node may compromise its confidentiality and privacy. The RBF-NN is slow in convergence.

based on Kalman filter is proposed in [123]. Here the reputation values received from different nodes are aggregated in the feedback system in Kalman filter. Kalman filter also produces the prediction variance. This variance is used to predict the reputation of the target node.

A trust prediction algorithm based on the concepts of trust mirroring and trust teleportation is proposed in [124]. In trust mirroring, the environment, interest and competency similarities of people are interpreted directly as an indicator for future trust. For example, node a observes that node b has similar interests and opinion on events based on past interactions then node a tends to trust the future behaviours of node b. In trust teleportation, if we assume node a has established trust relationship with b in the past, then all other nodes having similar interests and capabilities of b may become similarly trusted by a in the future.

A trust prediction scheme based on Resnick's prediction formula is proposed in [125]. The reliability of a partner to deliver accurate recommendations in the past is used as an important factor in the trust predictions. That is, if a node made significant amount of accurate predictions in the past, then he/she can be viewed as more trustworthy than another node that has made many poor predictions.

A trust prediction based on mathematical induction is proposed in [126]. Authors propose strategies to model the fluctuations of trust which is essentially used in predicting the trust value. There are two strategies proposed. The first strategy is to formally model the fluctuations of trust to formalize the dependency of trust on past experiences and trust representation for future. The second strategy is to formally model the fluctuations of trust in an inductive manner by a mathematical function relating a current trust representation and a current experience to the future trust representation.

[127] uses Radial Basis Function-Neural Network (RBF-NN) to estimate the reputation of nodes based on their internal attributes as opposed to their observed activity. Here the nodes are determined/identified with set of parameters. Each node is assumed to be aware of the initial setting parameter of the target

Table VII
INFLUENCE OF VARIOUS NETWORK DYNAMICS ON THE TRUST DYNAMICS

Trust Dynamics	Advantages	Disadvantages	Impact of network dynamics on trust dynamics		
			Mobility	Network density	Link breakages
Trust propagation	Trust propagation can serve as a first level information to prepare a node to have interactions with any strange node. Propagation of trust can help nodes to form a sub group and jointly combat the misbehaving activities.	Propagation has to be controlled by efficient algorithms otherwise it will lead to additional over heads.	Mobility helps to propagate the trust naturally [128]. The more mobility the quicker will be the propagation of trust.	More dense the network is, more faster will be the trust propagation as the connectivity increases with density.	Link breakage makes the trust propagation worse. More volatile the link more severe its effect on propagating the trust information.
Trust aggregation	Aggregation improves accuracy on the trust estimation. More the data for aggregation more will be the accuracy.	Complex aggregation algorithms may increase computational burden.	There are more chances of collecting more trust data for aggregation as the mobility increases.	Aggregation also improves with the node density as more data will be available for aggregation when the network density increases.	Link breakage affects the trust aggregation. Because, when the link breaks it is hard to collect enough samples for aggregations.
Trust prediction	Trust predictions help the node to be cautious to avoid any potential danger while communicating with strange nodes.	In most of the prediction algorithms, accuracy depends on the number of samples available. This demands more memory on nodes.	Mobility may weaken the trust prediction as it will be difficult to track the behaviour as the nodes move away.	More dense the network more samples available for prediction hence the prediction improves with the network density.	Link breakage affects the trust prediction. Because, when the link breaks it is hard to predict the performance as it may be because of link volatility or due to node's behaviour.

node. Now based on various attacks on the target node, the trustor node adjusts its opinion parameters on target node using some mathematical tools. These adjusted parameters will be used in RBF-NN to predict the future behaviour of the target node.

A detailed comparison of various trust predictions schemes used in MANETs trust management system is provided in Table VI.

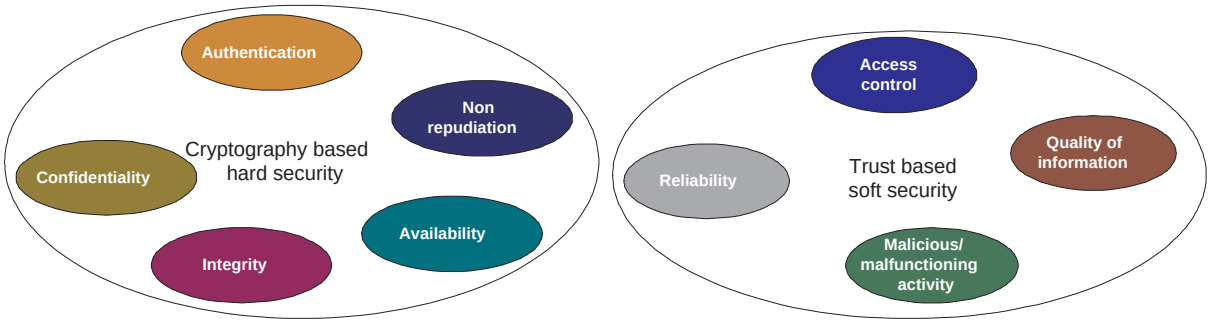
Summary:

Propagation, aggregation and prediction of trust are considered to be a winning combination as it solves some of the important issues at a minimal cost. Using these combination a trustor node can calculate accurately the trust value on future behaviour of target node though they are far apart. This will highly help the trustor node to have secure communications with the target node.

MANETs are highly dynamic networks. The connectivity, neighbourhood and association change continuously in this network and hence the trust and its dynamics. Some of the network dynamics are: mobility, network density, link breakages. Table VII gives the broad summary of influence of above listed network dynamics on the trust dynamics.

V. APPLICATION OF TRUST IN SECURITY

Applications of trust management is enormous in mobile networks [20]. In this section we analyze one of the important application namely network security. There are various means to provide network security. However, cryptography is one of the most explored and widely deployed way of providing security services. Cryptographic measures are often classified as hard security measures [16], [75] which



(a) Cryptography based hard security services

(b) Trust based soft security services

Figure 8. Pictorial representation of the hard and soft security services

provide partial security solutions by enabling data confidentiality, integrity, node authentication and non-repudiation. The hard security components are shown in Fig 8. a. Hard security is one time binary type solution where nodes either pass the security check or fail. In some situation nodes can behave as legitimate participants in the initial stage in a collaborative group and therefore pass the traditional cryptographic security checks. However, they could turn out to be selfish players and report false measurements either with malicious intentions or due to faulty components. Hard security scheme cannot help in detecting/preventing these kind of behaviours as these behaviours are continuously changing. Binary type of solution will not be effective. In addition reliability/trustworthiness of the information received from nodes, quality of information assessment and providing various levels of access control cannot be done effectively through hard security. The category of threat which are purely due to node behaviours are classified as soft security [16], [75]. Soft security components are shown in Fig. 8. b. Soft security threats can be most effectively handled using trust management systems [17], [129]. Trust management cannot be seen as a complete replacement for cryptography, rather a supplement to it. Cryptography and trust managements can work together to provide holistic security solution in MANET.

In this section, we review some of the literature handling soft security services such as malicious node detection, quality of information assessment, node reliability/trustworthiness using trust based approach. Though trust mechanisms can also be used in cryptography based hard security to improve its effectiveness [130]–[133] we skip that here as cryptography requires infrastructure for key management which is hard to achieve in MANET.

Trust and soft security:

A malicious node detection mechanism based on trust computations for wireless adhoc network is proposed in [134]. In this approach a trust authority collects the complaint reports (alarms) from users about the neighbours malicious activities. Trust authority integrates its direct observations on malicious node with the complaint reports it received from authenticated devices to create a global reputation vector. This vector will be distributed by the agent to all members of the network. Authenticated nodes aggregate the global trust vector received from the trust agent with their local trust vector to decide what level of trust to assign to a device. Malicious nodes will be detected whenever this trust level drops below a certain threshold.

A trust-based misbehavior detection and secure routing model known as Secure MANET Routing with Trust Intrigue (SMRTI) is proposed in [135]. A similar approach of hybrid trust evaluation as in [134] is followed here. SMRTI applies the trust prediction strategy and then decide whether to forward the packet to the neighbour node or pass that particular neighbour node. A similar work on the malicious

node detection using trust evaluations has been proposed in [136].

There has been a considerable work on the network trust and information security. The trust level of nodes play inevitable role in assessing the information trustworthiness. The underlined assumption is that if we know the history of information such as origin and details of the nodes who processed it (provenance details) then we can evaluate the information trust and node level trust. We highlight some recent work on the provenance based information trust evaluation in this section.

An agent-based approach to manage the trustworthiness of information in a dynamic information sharing environment is presented in [137]. In this model, information is stored and made available in the form of information objects, which consist of meta data and payload. The meta data defines a set of attributes of an information object including the origin history of the data (provenance). Using the meta data provenance graph for a derived information object can be built, which is used to determine whether two trust assessments are independent or not. Dempster-Shafer theory is then used for evaluating the trustworthiness of information objects.

Another data provenance trust model which estimates the level of trustworthiness of both information and information providers by assigning trust scores to them is proposed in [138]. Various aspects that may affect the trustworthiness of the data have been taken into account, which are (1) data similarity, (2) path similarity, (3) data conflict and (4) data deduction. An information item is likely to be true if it is provided by trustworthy node and node is trustworthy if it provides true information most of the time. Based on such inter-dependency an iterative procedure is developed to compute the trust scores of information.

Information trust assessment based on path and information similarity is proposed in [83]. The idea is that when the information item received from totally disjoint paths and the information contents are similar, then it is highly likely that the information is trustworthy and also all the nodes which processed the information are trustworthy. A feedback mechanism is presented to adaptively adjust the trust value of nodes based on the information trustworthiness evaluated at the receiver.

The trustworthiness evaluation model that presented in [138] is vulnerable to collusion attacks [139]. Majority rule based technique to detect the malicious colluding parties is proposed in [139]. $C_0, \ldots, C_i$ are assumed to be the clusters of information items which provide some evidences for an event E. If the average trust score of C_k $(0 \leq k \leq i)$ is larger than the average trust scores of any other clusters, then the information items in C_k are assumed to be correct, and the information items in the other clusters are incorrect. Based on this detection, penalty functions are proposed to reduce the trust scores of nodes that generated the colluding evidence items.

Some open research issues on provenance based information trust analysis have been pointed out in [140].

VI. Conclusion and Future Work

Trust and its management are exciting fields of research. The rich literature growing around trust give us a strong indication that this is an important area of research. Trust as a concept has a wide variety of adaptations and applications, which causes divergence in trust management terminology. The goal of this paper is to provide MANETs designers with multiple perspectives on the concept of trust, an understanding of the properties that should be considered in developing a trust metric, and insights on how trust can be computed. We started this paper by presenting various definitions of trust and metrics used for evaluating trust. We then presented a comprehensive survey of various trust computing approaches, their comparisons with respect to various attack models and computational requirements. We analyzed various literature on the trust dynamics such as trust propagation, aggregation and predictions. Finally we have provided a section detailing the application of trust mechanisms in security.

The trust schemes presented in this study cover a wide range of application and are based on many different types of mechanisms. There is no single solution that will be suitable in all contexts and

applications. While designing a new trust system, it is necessary to consider the constraints and the type of information that can be used as input by the network. A general observation is that so far, the existing research work and proposals lack completeness. There are important issues yet to be addressed. Some of them include:

- **Impact of network dynamics on trust:** Though, we have given a brief outline about impact of network dynamics on the various trust dynamics, the detailed analysis of the impact has to be addressed. For example, mobility can impact the trust propagations and various other security paradigms. But the clear quantifiable relationship is yet to be determined. Similarly, the relationship between other network dynamics (including link dynamics, network density) and trust and its dynamics are yet to be analyzed.
- **Computations of trust in cooperative and noncooperative games:** In a self organized distributed network, nodes can give positive or negative recommendations about others either genuinely or maliciously with some self interest. These aspects are analogous to situations in complex systems with game theoretic interactions [141]. The games can be non cooperative where every node plays game independently or cooperative where a set of nodes form sub groups and play game together against the rest of nodes [142]. Non cooperative games are tractable using Nash equilibrium [143]. Trust computation with cooperative game is not well analyzed yet. The earlier attempts are preliminary in nature and these attempts exploits the collaborations in positive way to obtain the trust scores [142].
- **Impact of heterogeneous nodes on trust:** Wireless networks could be highly heterogeneous. The heterogeneity could be in terms of the roles of the nodes, their inherent capability and security. Heterogeneity implies that not all nodes or their contents can be treated equally when it comes to trust evaluations. Thus, the same functional descriptions will not be applied to evaluate the trust levels of all nodes and their information. Investigation is needed on incorporating network dynamics and heterogeneity in the trust evaluation functions.
- **Security paradigms to enhance trust in the network:** The data delivery capabilities and security properties of the network directly impact the level of trust a recipient places on the information received. As an example, it is possible that a piece of information cannot be fully trusted unless its source and the path over which it is received are authenticated. If authentication services are not available one must decide whether to have the untrusted information or none at all. Further research is required to characterize these metrics through modelling efforts and to determine the degree to which security properties influence the network trust.
- **Social and context dependent trust:** Social relationship and context based trust by establishing social communities among entities has received considerable attention in recent days [144]. However, this is still unexplored area with respect to MANET. The complex dependence between the communications network, the social network, and the application network is not yet explored in MANET. The social communities can also help in validating the trust measurements. Validation of measured trust is another major area of future research.

We hope that the near future will bring consolidation around a set of fundamental principles for building trust and its various related issues, and that these will be realized in practical and commercial applications.

ACKNOWLEDGEMENT

This work was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official polices, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copy right notation here on.

REFERENCES

[1] V. Cahill., et al., "Using trust for secure collaboration in uncertain environments," *IEEE Pervasive Computing*, vol. 2(3), pp. 52–61, 2003.

[2] C. English, W. Wagealla, P. Nixon, S. Terzis, H. Lowe and A. McGettrick, "Trusting collaboration in global computing systems," *Lecture notes in computer science, Springer-Verlag*, vol. 2692, pp. 136–149, 2003.

[3] M. Deutch, "Cooperation and trust: Some theoretical notes," *Nebraska Symposium on Motivation, Nebraska University Press*, pp. 275–319, 1962.

[4] J. H. Cho, A. Swami and I. R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in *International Symposium on Trusted Computing and Communications, Trustcom*, pp. 641–650, 2009.

[5] A. Boukerch, L. Xu and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, no. 30, pp. 2413–2427, 2007.

[6] L. Kagal, T. Finin and A. Joshi, "Trust-based security in pervasive computing environments," *IEEE Computer*, vol. 34, pp. 154–157, 2001.

[7] H. Sarvanko, M. Hyhty, M. Katz and F. Fitzek, "Distributed resources in wireless networks: Discovery and cooperative uses," in *4th ERCIM eMobility Workshop in conjunction with WWIC 2010*.

[8] M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol," in *International Symposium on Trusted Computing and Communications, Trustcom*, pp. 802–808, 2009.

[9] V. Lenders, E. Koukoumidis, P. Zhang and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations," in *HotMobile '08: Proceedings of the 9th workshop on Mobile computing systems and applications*, pp. 60–64, 2008.

[10] B. J. Chang, and S. L. Kuo, "Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, May 2009.

[11] K. Avrachenkov, D. Nemirovsky and K. S. Pham, "A survey on distributed approaches to graph based reputation measures," in *The 2nd international conference on performance evaluation methodologies and tools*, pp. 1–9, 2007.

[12] M. Momani, "Trust models in wireless sensor networks: A survey," *Recent Trends in Network Security and Applications: Communications in Computer and Information Science*, vol. 89, no. 1, pp. 37–46, 2010.

[13] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Itrust 2005, number 3477 in lecture notes on computer science*, 2005.

[14] J. H. Cho and A. Swami, "Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks," in *14th International command and control research and technology symposium*, 2009.

[15] M. A. Azer, S. M. El-Kassas, A. W. F. Hassan, M. S. El-Soudani, "A survey on trust and reputation schemes in ad hoc networks," in *Third international conference on availability, reliability and security, ARES 08*, pp. 881–886, 2008.

[16] 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.

[17] 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.

[18] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Commun. Surveys Tuts.*, vol. 3, pp. 2–16, 2000.

[19] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 4, pp. 78–93, 2008.

[20] J. H. Cho, A. Swami, and I.R. Chen, "A survey of trust management in mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, 2011.

[21] D. H. Mcknight and N. L. Chervany, "The meanings of trust: University of Minnesota, Technical reports." http://misrc.umn.edu/wpaper/WorkingPapers/9604.pdf, 1996.

[22] J. Hassan, H. Sirisena, and B. Landfeldt, "Trust-based fast authentication for multiowner wireless networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 2, pp. 247–261, 2008.

[23] D. Q. Nguyen, L. Lamont and P. C. Mason, "On trust evaluation in mobile ad hoc networks," *Security and privacy in mobile information and communication systems, Springer*, vol. 17, pp. 1–13, 2009.

[24] J. D. Lewis and A. J. Weigert, "Trust as a social reality. Social Forces," *Social Atomism, Holism, and Trust. The Sociological Quarterly*, no. 63(4), pp. 967–985, 1985.

[25] S. P. Shapiro, "The social control of impersonal trust," *American Journal of Sociology*, vol. 93(3), pp. 623–658, 1987.

[26] J. B. Rotter, "A new scale for the measurement of interpersonal trust," *Journal of Personality*, vol. 35(4), pp. 651–665, 1967.

[27] J. G. Holmes, "Trust and the appraisal process in close relationships," *In Jones, W. H. and Perlman, D. (Eds.), Advances in personal relationships*, vol. 2, pp. 57–104, 1991.

[28] O. E. Williamson, "Calculativeness, trust, and economic organization," *Journal of Law and Economics*, vol. 34, pp. 453–502, 1993.

[29] P. Sztompka, "Trust: A sociological theory," in *Cambridge: Cambridge University Press*, 1999.

[30] R. C. Mayer, J. H. Davis and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, pp. 709–734, 1995.

[31] D. J. McAllister, "Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations," *Academy of Management Journal*, no. 38, pp. 24–59, 1995.

[32] L. Ding, P. Kolari, S. Ganjugunte, T. Finin, A. Joshi, "Modeling and evaluating trust network inference," in *Workshop on Deception, Fraud and Trust in agent societies at the Third international joint conference on autonomous agents and multi-agent systems, AAMAS'04*, pp. 21–32, July, 2004.

[33] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in *The ACM workshop on New security paradigms*, pp. 48–60, 1998.

[34] G. Elofson, "Developing trust with intelligent agents: An exploratory study," in *The First International Workshop on Trust*, pp. 125–139, 1998.

[35] R. Falcone, G. Pezzulo, and C. Castelfranchi, "A fuzzy approach to a belief-based trust computation," in *Lecture Notes on Artificial Intelligence*, pp. 73–86, 2003.

[36] C. Castelfranchi and R. Falcone, "Trust is much more than subjective probability: Mental components and sources of trust," in *The 33rd Hawaii International Conference on System Sciences*, 2000.

[37] D. Olmedilla, O. Rana, B. Matthews, W. Nejdl, "Security and trust issues in semantic grids," in *Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies*, vol. 05271, 2005.

[38] D. Gambetta, "Can we trust trust?," *Trust: Making and Breaking Cooperative Relations Gambetta, D (ed.). Basil Blackwell. Oxford*, pp. 213–237, 1990.

[39] A. Jøsang, S. Marsh, and S. Pope, "Exploring different types of trust propagation," *Lecture notes in computer science, Springer-Verlag*, pp. 179–192, 2006.

[40] T. Yu, M. Winslett, K. E. Seamons, "Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation," *ACM Transactions on Information System Security*, vol. 6(1), pp. 1–42, 2003.

[41] L. Mui, M. Mohtashemi and A. Halberstadt, "A computational model of trust and reputation," in *Proceedings of the 35th Hawaii International Conference on System Science, HICSS'02*, 2002.

[42] G. Theodorakopoulos and J. S. Baras, "A testbed for comparing trust computation algorithms." http://infoscience.epfl.ch/record/111326/files/gtjb-asc06a.pdf.

[43] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," *Volume 875 Lecture notes in computer science*, pp. 3–18, 1994.

[44] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "Eigenrep: Reputation management in P2P networks," in *World-Wide Web Conference*, 2003.

[45] R. Sherwood, S. Lee, and B. Bhattacharjee, "Cooperative peer groups in NICE," *Comput. Netw.*, vol. 50, no. 4, pp. 523–544, 2006.

[46] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad-hoc networks," in *IEEE International conference on communications, ICC 2008*, pp. 2129–2133.

[47] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust in peer-to-peer communities," *IEEE Transactions on Knowledge and Data Engineering, Special Issue on Peer-to-Peer Based Data Management*, vol. 16, no. 7, pp. 843–857, July 2004.

[48] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in *The 3rd ACM workshop on Wireless security, WiSe '04*, pp. 1–10, 2004.

[49] A. Jøsang, "An algebra for assessing trust in certification chains," in *The Network and Distributed Systems Security Symposium NDSS 99*, 1999.

[50] G. Lenzini, M. S. Bargh and B. Hulsebosch, "Trust-enhanced security in location-based adaptive authentication," *Electronic Notes in Theoretical Computer Science*, no. 197, pp. 105–119, 2008.

[51] R. Haenni, "Using probabilistic argumentation for key validation in public-key cryptography," *International Journal of Approximate Reasoning*, vol. 38(3), pp. 355–376, 2005.

[52] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," in *Proceedings of the 13th International Conference on Parallel and Distributed Systems*, pp. 1–8, 2007.

[53] C. Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas, "Robust cooperative trust establishment for MANETs," in *The fourth ACM workshop on security of ad hoc and sensor networks*, pp. 23–34, 2006.

[54] A. Jøsang and R. Ismail, "The beta reputation system," in *Proc. BCEC*, pp. 324–337, 2002.

[55] T. Wen, H. Jianbin and C. Zhong, "Research on a fuzzy logic-based subjective trust management model," *Journal of Computer Research and Development*, no. 42(10), pp. 1654–1659, 2005.

[56] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Comput. Netw.*, vol. 53, no. 14, pp. 2396–2407, 2009.

[57] V. S. Grishchenko, "A fuzzy model for context-dependent reputation," in *Proceedings of Trust, Security and Reputation Workshop at ISWC*, 2004.

[58] F. Azzedin, A. Ridha and A. Rizvi, "Fuzzy trust for Peer-to-Peer based systems," *World Academy of Science, Engineering and Technology*, pp. 123–127, 2007.

[59] J. A. Golbeck, "Computing and applying trust in web-based social networks," in *University of Maryland at College Park (2005)*.

[60] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and distrust values," in *IFIP International Conference on Trust Management-2010*, pp. 157–171.

[61] S. Choudhury, S. D. Roy and S. A. Singh, "Trust management in ad hoc network for secure DSR routing," *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics*, pp. 496–500, 2008.

[62] J.-W. Ho, "Zone-based trust management in sensor networks," in *IEEE International Conference on Pervasive Computing and Communications*, pp. 1–2, 2009.

[63] A. A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks," *Wireless Personal Communications*, vol. 37(1-2), pp. 139–168, 2006.

[64] S. Buchegger and J. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *In Proc. 2nd Workshop on Economics of Peer-to-Peer Systems*, 2004.

[65] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 1–10, 2005.

[66] T. Jiang and J. S. Baras, "Trust evaluation in anarchy: A case study on autonomous networks," in *25th IEEE International Conference on Computer Communications, INFOCOM'06*, pp. 1–12, April 2006.

[67] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 318–328, February 2006.

[68] Z. Liu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," in *IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS'04*, pp. 80–85, May 2004.

[69] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying trust in mobile ad-hoc networks," in *International Conference on Integration of Knowledge Intensive Multi-Agent Systems*, pp. 65–70, April 18-21, 2005.

[70] P. B. Velloso, R. P. Laufer, D. O. Cunha, O. C. M. B. Duarte and G. Pujolle1, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Netw. Service Manag.*, vol. 7, no. 3, pp. 172–185, Sep. 2010.

[71] J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in *Proceedings of 2nd International Conference on Trust Management*, March 2004.

[72] V. Balakrishnan, V. Varadharajan, U. K. Tupakula and P. Lucs, "Trust and recommendations in mobile ad hoc networks," in *Proceedings of 3rd International Conference on Networking and Services (ICNS 2007)*, pp. 64–69, 2007.

[73] Y. L. Sun, Z. Han, W. Yu and K. J. Ray Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *IEEE International Conference on Computer Communications, INFOCOM'06*, pp. 1–13, April 2006.

[74] Y. Sun, W. Yu, Z. Han and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb 2006.

[75] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *In Proceedings of First International Joint Conference on Autonomous Agents and Multiagent Systems*, pp. 294–301, 2002.

[76] P. Chatterjee, I. Sengupta and S. K. Ghosh, "A distributed trust model for securing mobile adhoc networks," in *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 818–825, 2010.

[77] N. Wilson, "Algorithms for Dempster-shafer theory," in *Algorithms for Uncertainty and Defeasible Reasoning*, pp. 421–475, Kluwer Academic Publishers, 2000.

[78] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems," in *Proc. 20th International Joint Conference on Artificial Intelligence, IJCAI'07*, pp. 1551–1556, 2007.

[79] C. Hang, Y. Wang, and M. P. Singh, "An adaptive probabilistic trust model and its evaluation," in *The 7th International Joint Conference on Autonomous Agents and MultiAgent Systems, AAMAS'08*, pp. 1485–1488, May 2008.

[80] A. Jsang, "A subjective metric of authentication," *Lecture notes in computer science, Springer-Verlag*, vol. 1485/1998, pp. 329–344, 1998.

[81] R. Zhou and K. Hwang, "Trust overlay networks for global reputation aggregation in p2p grid computing," in *20th International Parallel and Distributed Processing Symposium, IPDPS 2006*, April 2006.

[82] E. Damiani, D. C. D Vimercati, S. Paraboschi, P. Samarati and F. Violante, "A reputation-based approach for choosing reliable resources in peer-to-peer networks," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pp. 207–216, 2002.

[83] X. Wang, K. Govindan and P. Mohapatra, "Provenance based information trustworthiness evaluation in multi-hop networks," in *IEEE Global Communication Conference, Globecom-10*, 2010.

[84] S. S. Park, J. H. Lee, and T. M. Chung, "Cluster-based trust model against attacks in ad-hoc networks," in *Third International Conference on Convergence and Hybrid Information Technology*, pp. 526–532, 2008.

[85] A. Boukerche and Y. Ren, "A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks," in *Proceedings of the 5th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pp. 88–95, 2008.

[86] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in *IEEE International Conference on Communications, ICC '08*, pp. 2129 – 2133, 19-23 May 2008.

[87] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in *12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, pp. 411–414, 2006.

[88] B. Lagesse, M. Kumar, J. M. Paluska and M. Wright, "DTT: A distributed trust toolkit for pervasive systems," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications*, pp. 1–8, 2009.

[89] J. Li, N. Li, X. Wang and T. Yu, "Denial of service attacks and defenses in decentralized trust management," in *Securecomm and Workshops, 2006*, pp. 1–12.

[90] C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems," in *The twenty first international conference on Information systems, ICIS '00*, pp. 520–525, 2000.

[91] L. F. Perrone and S. C. Nelson, "A study of on-off attack models for wireless ad-hoc networks," in *First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks*, 2006.

[92] Y. L. Sun, Z. Han, W. Yu and K. J. Ray Liu, "Attacks on trust evaluation in distributed networks," in *IEEE Internaional Conference on Information Sciences and Systems, CISS*, March 2006.

[93] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *The 3rd international symposium on Information processing in sensor networks, IPSN '04*, pp. 259–268, 2004.

[94] J. R. Douceur, "The sybil attack," in *First International Workshop on Peer-to-Peer Systems, IPTPS '01*, pp. 251–260, 2002.

[95] J. D. Microsoft, J. R. Douceur, and J. S. Donath, "The sybil attack," in *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, pp. 251–260, 2002.

[96] H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, "Dsybil: Optimal sybil-resistance for recommendation systems," in *SP '09: Proceedings of the 30th IEEE Symposium on Security and Privacy*, pp. 283–298, 2009.

[97] J. Lopez, R. Romana, I. Agudoa, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *Computers & Security*, vol. 28, no. 7, pp. 545–556, 2009.

[98] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *WWW '03: Proceedings of the 12th international conference on World Wide Web*, pp. 640–651, 2003.

[99] P. B. Velloso, R. P. Laufer, O. C. M. B. Duarte, and G. Pujolle, "A trust model robust to slander attacks in ad hoc networks," in *IEEE International Conference on Computer Communications and Networks (ICCCN08) Workshop*, 2008.

[100] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[101] M. N. Lima, A. L. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks.," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 66–77 , 2009.

[102] T. R. Andel, A. Yasinsac, "Surveying security analysis techniques in manet routing protocols," *IEEE Commun. Surveys Tuts.*, 2007.

[103] D. Quercia, S. Hailes and L. Capra, "Lightweight distributed trust propagation," in *The Seventh IEEE International Conference on Data Mining*, pp. 282–291, 2007.

[104] E. Gray, J. marc Seigneur, Y. Chen, and C. Jensen, "Trust propagation in small worlds," in *Proc. of 1st Int. Conf. on Trust Management, iTrust03*, pp. 239–254, 2003.

[105] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," in *Security Protocols Workshop*, vol. 2845, pp. 47–66, April 2002.

[106] S. Trifunovic, F. Legendre and C. Anastasiades, "Social trust in opportunistic networks," in *INFOCOM IEEE Conference on Computer Communications Workshops*, pp. 1–6, 2010.

[107] D. Ingram, "An evidence based architecture for efficient, attack-resistant computational trust dissemination in Peer-to-Peer networks," in *Proceeding of 3rd International Conference on Trust Management, Lecture notes on computer science, Volume 3477*, pp. 273–288, 2005.

[108] S. Capkun, J. P. Hubaux and L. Buttyan, "Mobility helps security in ad hoc networks," in *The 4th ACM international symposium on Mobile ad hoc networking, Mobihoc'03*, pp. 46–56, 2003.

[109] N. Cheng, K. Govindan and P. Mohapatra, "Rendezvous based trust propagation to enhance distributed network security," in *INFOCOM-2011 Workshops SCNC*, 2011.

[110] M. Detyniecki, "Mathematical aggregation operators and their application to video querying," in *PhD thesis, Computer Science Department of the University Pierre and Marie Curie (UPMC) - Paris, France*, 2000.

[111] T. Calvo, G. Mayor and R. Mesiar (eds.), "Aggregation operators," *Physica-Verlag Springer-Verlag*, 2002.

[112] Y. Wang and M. P. Singh, "Trust representation and aggregation in a distributed agent system," in *The 21st national conference on Artificial intelligence, AAAI'06*, pp. 1425–1430, 2006.

[113] H. Chen, H. Wu, X. Cao, and C. Gao, "Trust propagation and aggregation in wireless sensor networks," *Japan-China Joint Workshop on Frontier of Computer Science and Technology*, pp. 13–20, 2007.

[114] Y. Jin and M. Thielscher, "Iterated belief revision, revised," *Artif. Intell.*, vol. 171, no. 1, pp. 1–18, 2007.

[115] P. Pardo, "Aggregation of trust for iterated belief revision in probabilistic logics," *Lecture notes in computer science, Springer-Verlag*, pp. 165–179, 2009.

[116] Y. Bachrach, A. Parnes, A. D. Procaccia, and J. S. Rosenschein, "Gossip-based aggregation of trust in decentralized reputation systems," *Autonomous Agents and Multi-Agent Systems*, vol. 19, no. 2, pp. 153–172, 2009.

[117] D. Kempe, A. Dobra, and J. Gehrke, "Gossip-based computation of aggregate information," in *The 44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 482–491, 2003.

[118] J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," in *The 8th ACM Symposium on Identity and Trust on the Internet, IDtrust '09*, pp. 23–37, 2009.

[119] E. Damiani, S. D. C. Vimercati, P. Samarati and M. Viviani, "A WOWA-based aggregation technique on trust values connected to metadata," *Electronic Notes in Theoretical Computer Science*, vol. 157, no. 3, pp. 131–142, 2006.

[120] Y. Kim and K. Doh, "Trust type based semantic web services assessment and selection," in *Proc. of ICACT*, pp. 2048–2053, 2008.

[121] S. J. H. Yang, J. S. F. Hsieh, B. C. W. Lan, and J.-Y. Chung, "Composition and evaluation of trustworthy web services," in *BSN '05: Proceedings of the IEEE EEE05 international workshop on Business services networks*, pp. 5–12, 2005.

[122] L. Capra and M. Musolesi, "Autonomic trust prediction for pervasive systems," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications, AINA'06*, pp. 481–488, 2006.

[123] X. Wang, L. Liu and J. Su, "Rlm: A general model for trust representation and aggregation," *IEEE Transactions on Services Computing*, vol. 99, 2010.

[124] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers? Bootstrapping and prediction of trust," in *10th International Conference on Web Information Systems Engineering, WISE'09*, 2009.

[125] J. O'Donovan and B. Smyth, "Trust no one: Evaluating trust-based filtering for recommenders," in *International Joint Conference on Artificial Intelligence, IJCAI'05*, vol. 19, pp. 1663–1665, 2005.

[126] C. M. Jonker and J. Treur, "Formal analysis of models for the dynamics of trust based on experiences," in *MAAMAW '99: Proceedings of the 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World*, pp. 221–232, 1999.

[127] F. M. Ham, E. Y. Imana, A. Ondi, R. Ford, W. Allen and M. Reedy, "Reputation prediction in mobile adhoc networks using RBF neural networks," *Engineering Applications of Neural Networks Communications in Computer and Information Science, EANN, CCIS 43*, pp. 485–494, 2009.

[128] F. Li and J. Wu, "Mobility reduces uncertainty in MANETs," in *IEEE International Conference on Computer Communications, INFOCOM'07*, pp. 1946–1954.

[129] M. Carbone, M. Nielsen and V. Sassone, "A formal model for trust in dynamic networks," in *In Proc. of International conference on software engineering and formal methods, SEFM03*, pp. 54–63, 2003.

[130] E. Ngai and M. Lyu, "Trust- and clustering-based authentication services in mobile ad hoc networks," in *The 24th International Conference on Distributed Computing Systems Workshops*, pp. 582–587, March 2004.

[131] Y. P. Chen and A. L. Liestman, "A zonal algorithm for clustering ad hoc networks," *International Journal of Foundations of Computer Science, IJFCS*, 2003.

[132] P. R. Zimmermann, *The official PGP user's guide*. Cambridge, MA, USA: MIT Press, 1995.

[133] G. Wang, Q. Wang, J. Cao, and M. Guo, "An effective trust establishment scheme for authentication in mobile ad hoc networks," in *CIT '07: Proceedings of the 7th IEEE International Conference on Computer and Information Technology*, pp. 749–754, 2007.

[134] D. McCoy, D. Sicker and D. Grunwald, "A mechanism for detecting and responding to misbehaving nodes in wireless networks," in *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON '07*, pp. 678–684, 2007.

[135] V. Balakrishnan, V. Varadharajan, P. Lucs, and U. K. Tupakula, "Trust enhanced secure mobile ad-hoc network routing," in *21st International Conference on Advanced Information Networking and Applications Workshops, AINAW '07*, pp. 27–33, 2007.

[136] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu and K. Y. Lam, "Trust based malicious nodes detection in MANET," in *International Conference on E-Business and Information System Security, EBISS '09*, pp. 1–4, 2009.

[137] B. Yu, S. Kallurkar, G. Vaidyanathan, and D. Steiner, "Managing the pedigree and quality of information in dynamic information sharing environments," in *The 6th ACM international joint conference on Autonomous agents and multiagent systems AAMAS '07*, pp. 1–3, 2007.

[138] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in *SDM '08: Proceedings of the 5th VLDB workshop on Secure Data Management*, pp. 82–98, 2008.

[139] C. Dai, H.-S. Lim, E. Bertino, and Y.-S. Moon, "Assessing the trustworthiness of location data based on provenance," in *The 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, GIS'09*, pp. 276–285, 2009.

[140] E. Bertino, C. Dai, and M. Kantarcioglu, "The challenge of assuring data trustworthiness," in *DASFAA '09: Proceedings of the 14th International Conference on Database Systems for Advanced Applications*, (Berlin, Heidelberg), pp. 22–33, Springer-Verlag, 2009.

[141] J. Baras and T. Jiang, "Cooperative games, phase transitions on graphs and distributed trust in MANET," in *43rd IEEE Conference on Decision and Control*, vol. 1, pp. 93–98, 2004.

[142] J. S. Baras and T. Jiang, “Cooperation, trust and games in wireless networks,” in *Proceedings of Symposium on Systems, Control and Networks*, pp. 183–202, 2005.
[143] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini and R. R. Rao, “Cooperation in wireless adhoc networks,” in *Proceedings of IEEE INFOCOM*, pp. 808 – 817, 2003.
[144] W. S. Chow and L. S. Chan, “Social network, social trust and shared goals in organizational knowledge sharing,” *Information & Management*, vol. 45, no. 7, pp. 458–465, Nov. 2008.