A Systematic Analysis of Trust Dynamics and Trust Computations in Wireless Ad Hoc Networks

Dr.B. Prabhakar Reddy, P. Imran Khan, S. Mahaboob Basha

Professor[1], Assistant Professor[2,3]
1,2Bheema Institute of Technology and Sciences, Adoni-518301

[3]Geethanjali College of Engineering and Technology, Kurnool.

Abstract
In mobile ad hoc networks (MANETs), trust is crucial. It helps organizations deal with the risks and challenges that come with relying on the actions of free agents. Complexity limitations in processing, as well as the free mobility of individual nodes, make trust calculations and management particularly difficult in MANETs. This precludes the use of methods developed for use on different networks. A malicious node in a MANET has the potential to do serious harm and compromise data integrity. As a result, the certainty with which an entity transacts with a node is improved by analysis of the node's trust level. Specifically for mobile ad hoc networks (MANETs), we give a comprehensive overview of many trust computing strategies. We focus on summarizing and contrasting these methods. We also examine the impact of trust on security services and the effects of trust propagation, prediction, and aggregation methods, as well as the effect of network dynamics on trust dynamics..

INTRODUCTION

In order for the MANET to accomplish its deployment goals, which may include sensing and event monitoring, distributed cooperation and sharing of information are seen as necessary processes. Only if everyone involved in a project can be trusted, can it be successful [1]-[3]. Due to the lack of a centralized control unit, MANETs are more vulnerable to tampering and malfunction when used in harsh or uncontrolled situations. Because of these traits, a component node must exercise caution while cooperating or interacting with other nodes, as the behavior of nodes varies over time and in response to their surroundings. As a result, trust between nodes must be established and quantified for MANET to function as intended. This is especially crucial in social networks and tactical networks involving allied states [4] where a large number of diverse organizations join and a high degree of coordination is necessary. Nodes' operations, sensing capacities, and other relevant behaviors may all exhibit heterogeneity. Access control, authentication, malicious node detections, and safe resource sharing are just some of the network security services that might benefit from using a trust system to evaluate the reliability of incoming data [5–8]. As a result, it is essential to regularly assess the credibility of individual nodes using a variety of metrics and computational techniques.

Because node behavior drives most of the variation in the trust value in static networks, trust computations there are rather straightforward. When enough data is collected, these patterns of behavior become obvious. Trust calculations, however, are difficult in MANET because to:

• MANETs can have varying degrees of mobility, from low (humans carrying sensors on foot) to high (sensors mounted on vehicles). Because of its transience, the make-up of the network might shift dramatically over time. When the neighbor is always changing, it's hard to keep tabs on them and gauge how trustworthy they are. If the location and time of the MANET nodes' readings can be determined, the resulting data will be more reliable and useful [9]. In contrast, K. Govindan and P. Mohapatra can be reached at gkannan, prasant@cs.ucdavis.edu> when they are affiliated with that department at that institution.

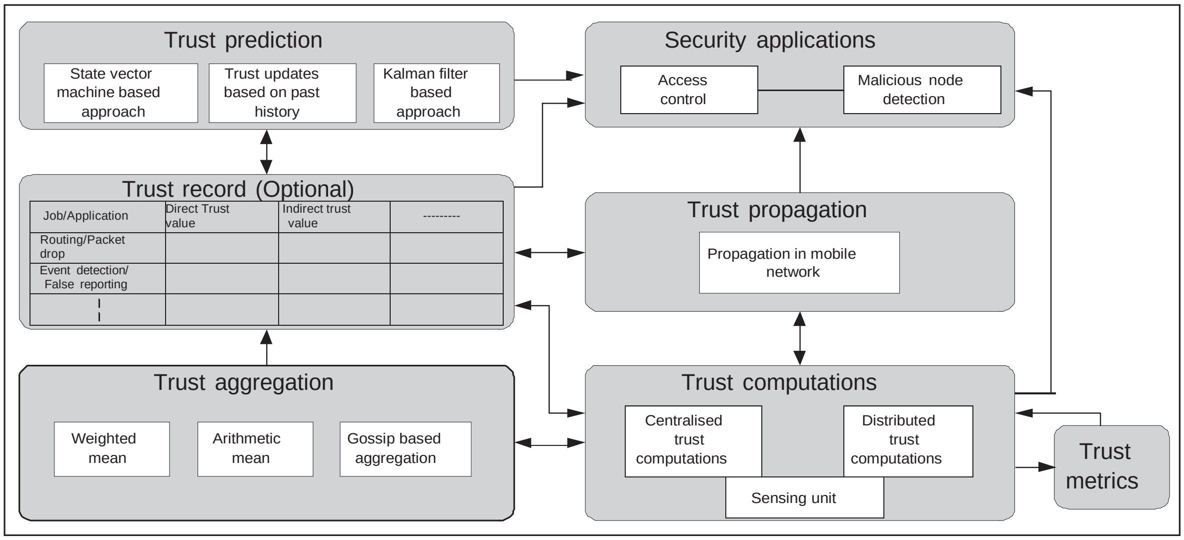


Figure 1. Relationship among various trust blocks

Constantly shifting locations make it difficult to tie together data and node activity. • Lack of a command hub makes it tough to keep tabs on how nodes are behaving. Without the hub, the complexity of trust calculations increases at an exponential rate. Obtaining a node's trustworthiness from another node in a network of N linked nodes has a worst-case complexity of O(N 2) [10].
There has been a lot of recent research into MANET-related trust computing approaches. Trust system designers would benefit greatly from a comprehensive overview and summary of these methods.

Trust in wireless sensor networks, social networks, internet applications, and cognitive networks is the subject of a number of research reviews [11–19]. However, there is a shortage of comprehensive studies on MANET management. In [20], a recent survey is presented on the topic of trust management in MANET. Metrics, attack models on trust management, and applications are only few of the topics covered in this study. There is a lack of a comprehensive review of trust computation techniques, trust dynamics, and their inter-operations in [20]. Given the abundance of literature in these domains, a unified study of these vital trust system components is warranted.

What we've added: In an effort to close this gap, this study presents a systematic review of the trust computation methodologies and trust dynamics relevant to MANET. The major trust dynamics that can aid in trust calculations include trust propagation, trust aggregation, and trust prediction. The functional blocks of our proposed MANET trust system are depicted in Fig. 1.

• Metrics and definitions-based trust calculations

Propagation, Aggregation, Prediction, and Applications of Trust

At first, we'll use various metrics and advice to determine the node's trustworthiness (trust computations). As demonstrated in Fig. 1's Trust calculations block, this trust computation can be managed centrally or in a decentralized manner. The network will be updated with these computed trust levels so that it may be properly established.

connects nodes that aren't physically close together. During trust propagation, the trust values of all possible pathways will be added together to produce a single trust value that may be saved in the past. Applications that require security will make use of the anticipated trust value, which was generated using the stored trust value. The trust value is not only utilized as input into the trust computation block, but also as feedback. As a result, our envisioned trust system has tight connections between computations, propagation, aggregation, and prediction blocks based on trust.

We have organized this survey using Fig. 1 as our guiding model. In Section II, we look at how trust is defined, measured, and measured for, as well as some of the attributes that are employed in computing trust. The various methods for computing trust are summarized in Section III. The available literature on trust dynamics is summarized in Section IV. Section V provides a literature review that focuses on the use of trust in security. Section VI provides a summary of the paper and some suggestions for future trust research.

I. Trust Definition, Metrics and Properties

It is vital to comprehend trust definition, metrics, and various trust attributes used in trust calculations in order to calculate the trust level on nodes.

A. Definition

In the written word, "trust" is defined in a variety of ways. Reliability, usefulness, availability, reputation, risk, confidence, and the quality of services are all indicators of trust. However, none of these ideas really captures the essence of what trust is. This is because trust is not a concrete idea but rather a mixture of several subtle elements [21].

Research on trust has been conducted in several fields, including the behavioral and social sciences, economics, politics, ethnography, and, most recently, wireless networks [22], [23]. The problem is viewed and addressed differently by each body of literature. For instance, some psychologists define trust as an individual perspective or trait [26], but sociologists often view it as relational in character [24, 25]. Trust is seen as an interpersonal phenomena by social psychologists [27] and a rational decision process to maximize its own utility by economists [28].

These definitions may be broken down into the following categories in the context of MANETs:

The definition of trust given by Morton Deutsch [3], which is more widely accepted than many others, states that trusting behavior 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. According to [29], [30], trust may be thought of as a wager on the unknowable behavior of others in the future.

2) Trust as conviction: Trust is the conviction that one may rely on the word, deed, and judgment of another person [31]-[37].

3) Trust as subjective probability: Trust (or mistrust) is the degree to which a person believes it is likely that another person would act in a certain way during a certain time frame and in a certain setting [16], [38]-[41].

Fourthly, trust is a binary connection with weights between two people in a network. Take, for instance, a hierarchically structured network of intelligence agents. One way to define trust is as the conviction of an authoritative figure (Person A) that a subordinate (Person B) will not be a double agent [42].

Summary:

In order to determine a node's trustworthiness, it is necessary to have a firm grasp on the concept of trust, as well as the metrics and qualities used to measure it.

Part A: Meaning

The term "trust" can be understood in many different ways depending on the context. Trust may be measured by a number of factors, including the quality of services, their utility, reliability, availability, reputation, risk, and confidence. However, none of these definitions really expresses the core concept of trust. This is due to the fact that trust consists of a number of intangible qualities rather than a single entity [21].

Various academic disciplines, from the arts and humanities to economics and politics to ethnography and, most lately, wireless networks [22], [23], have explored the topic of trust. Each corpus of literature offers a unique perspective on the issue and set of solutions. Trust, for instance, is typically viewed as relational in nature by sociologists [24, 25], but is defined as an individual perspective or attribute by certain psychologists [26]. Sociologists [27] and economists [28] both see trust in different ways: as an interpersonal phenomenon or as a logical decision process to maximize its own utility.

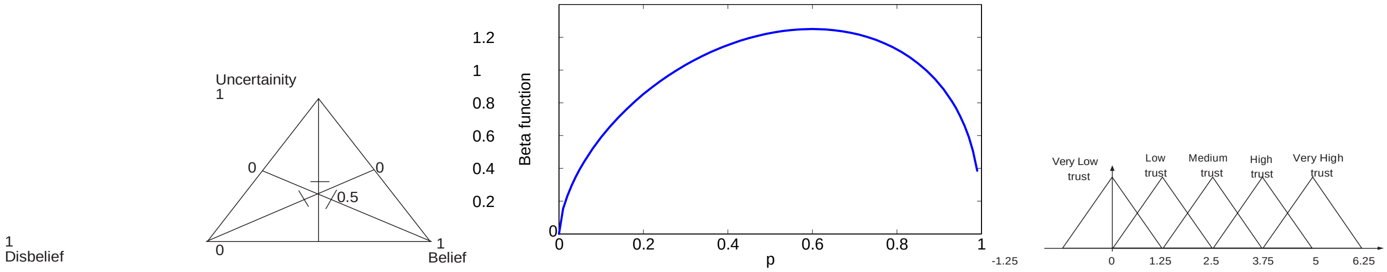
In the context of MANETs, we can classify these definitions as follows:

Trusting behavior 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. This definition of trust is more widely accepted than many others. Trust, as discussed in [29], [30], can be viewed as a bet on the unpredictable actions of people in the future.

2) Trust as conviction: Belief that another's word, conduct, and judgment may be relied upon [31]-[37].

Trust (or distrust) is the degree to which one thinks it plausible that another person will act in a specific way at a certain time and place [16], [38]-[41].

Fourth, in a network, trust is a two-way, bidirectional, weighted link between individuals. Consider a group of intelligent brokers organized in a hierarchical manner. The belief of a superior (Person A) in the loyalty of a subordinate (Person B) is one definition



(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

The degree to which a node is trusted indicates how confident the network is in the target node's promises to be truthful, reliable, capable, available, and provide high-quality service in the future. It also represents the reciprocal nature of the interactions between nodes, where each node acts in a trustworthy manner and communicates reliably only with other nodes that have earned a high degree of trust from the given node.

A. Metrics

Numerous scales and methodologies have been applied to the study of trust. The research on trust measurements may be broken down into the following sections:

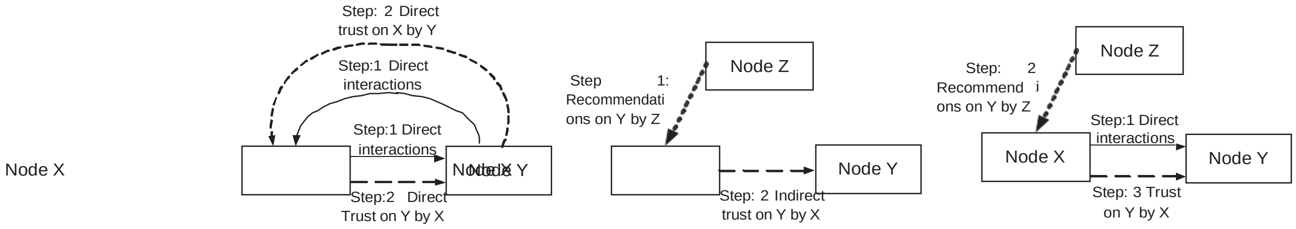
Some approaches utilize a trust scale with either continuous or discrete values. In [43]–[46], for instance, trust is characterized by a continuous value in [0, 1], but in [35], it is characterized by a discrete value in [1, 1]. There are various threshold-based methods for gauging trust's extent. For instance, in [47], a node is deemed reliable if its normalized quantity of pleasure relative to its interaction count is over some threshold.

Two) Elements of Trust Having both a trust value in the interval [0, 1] and a confidence value c in the interval [0, 1] denotes a node's reliability in [48]. The node's level of trust in the observed trust value is represented by the confidence value (C), while the trust value (T) is the value itself. Now, reliability is represented by the 2D rectangle coordinate that is closest to the origin (T, C). Where b, d, and u stand for confidence, unbelief, and uncertainty, respectively, the metric in [49], [50] is a triplet (b, d, u) [0, 1]3 b + d + u = 1. Fig. 2 depicts a trust representation in the form of a triplet space.

#3) Logics of trust (probability, fuzzy): Probability has been used as a measure of reliability in some of the methods. While [51], [52] rely on probability measures to establish confidence, [53] instead employs the ratio of successfully transferred packets to total packets received. In [54], Beta dispersion is employed. Here, the Beta distribution is utilized to calculate the trustworthiness based on the negative and good experiences. Figure 2b depicts the Beta distribution over a range of p, with the good experience factor = 1.7 and the poor experience factor = 1.3 held constant. The average of this distribution provides a measure of confidence.

The concept of trust is represented by fuzzy logics in certain works [35, [55]-[57]. Fuzzy logics employ labels (often adjectives) from everyday language to indicate a range of potential answers. A trust value in the range [1.25, 1.25] indicates an extremely low level of trust, for example, and so on. A node with a trust score of 0.25 is considered to have 75% extremely low trust and 25% low trust [58] in Fig. 2. c.

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


Node X
Step: 2 Direct trust on X by Y
Step:1 Direct interactions
Step:1 Direct interactions
Node X
Node Y
Step:2 Direct Trust on Y by X
Node Z
Step 1: Recommendations on Y by Z
Node Y
Step: 2 Indirect trust on Y by X
Node Z
Step: 2 Recommendations on Y by Z
Step:1 Direct interactions
Node X
Node Y
Step: 3 Trust on Y by X

(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

A. Trust properties

We next go on to discussing traits that are relevant for calculating trust. The three basic qualities of trust that hold in trust networks are asymmetry, transitivity, and compositionality, which we discuss based on [59], [60]. Because of this asymmetry, it is not certain that B will trust A to the same extent that A trusts B.

Because of the transitivity feature, trust may be transmitted from one trustworthy user to another. Since A trusts B and B trusts C, it follows that A also trusts C to some extent.

To be composable, trust data must be able to be combined from several sources to yield a single judgment.

II. TRUST COMPUTATIONS

Experience, suggestion, and knowledge are the three building blocks of trust calculations [61]. Each node's 'experience' with other nodes is quantified in real time by that node's nearest neighbors and recorded in the trust table. As a'recommendation' portion of the trust, the current trust table is broadcast to all other nodes. The 'knowledge' part of total trust is updated on a regular basis to incorporate the results of earlier evaluations of trust. These three factors may now be used singly or in tandem to determine the trustworthiness of a person or organization.

There are many major groups into which the research on trust calculations fits:

- Collaborative trust calculations Each node determines its own trustworthiness relative to its neighbors.

The node is managed and assisted by a centralized agent during trust calculations. In what follows, we provide a comprehensive account of the studies conducted on these topics.

Distributed trust computations

As illustrated in Fig. 3, there are three broad categories into which distributed trust calculations fall: neighbour sensing (Direct trust), recommendations based trust (Indirect trust), and a hybrid technique.

Sense of neighborhood (Indirect trust):

In Fig. 3a, we see an example of a distributed trust computation using neighbour sensing, in which each node keeps an eye on its neighbors to gather event reports, which it then stores in a 'knowledge' cache. One way to gauge a network's reliability is for a trustor node to compare its own report of an event's observations with those of other nodes.

received both from the trustee node (trust between nodes must be quantified) and from other neighboring nodes. The level of discrepancy between the observation reports will be used to establish a trust factor.
[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:

$$T = W(R_p) \times R_p + W(R_q) \times R_q + W(R_e) \times R_e + W(D) \times D \qquad (1)$$

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:

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

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 acknowledge- ment 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

$$\sum_n \frac{W_i}{W} x_i \qquad (3$$

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

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

The weighted variance is given by

$$\sigma_w^2 = \frac{\sum W_i^2 \, \sigma^2}{(\sum W_i)^2} \qquad (5)$$

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

$$q\_\_\_\_ \quad {}^2 \, \sigma_w \qquad (6)$$

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$c_{ij} \;/\!= c_{ji}$. 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 votingscheme. The effective confidence value between i and j is given by:

$$= \frac{c_{ij} + c_{ji}}{2} \quad (7)$$

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

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

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

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

where Ni is the total number of nodes in the compact interconnected network. As an alternative to using only Ni nodes' opinions for calculating trust, the authors suggest using a global voting mechanism.
In [67], the research from [66] is developed further. A directed trust graph G(V, E) was modeled for the assessment process, where nodes V represent entities and the strength of edges E reflect trust links (strong or weak). The goal of this approach is to streamline the trust and confidence values in multihop communication by combining them into a single opinion value. In [68], the authors suggest a trust-based threat-reporting system for MANETs. An IDS is built into each and every one of the nodes. The activity of each node's nearest neighbors is tracked, and a "trust report" is produced based on that information. At the outset, the degree of confidence each node has in the others is completely arbitrary. Once the trust report has been prepared, it will be sent out via a network broadcast or flooded in a controlled manner. If a node is sending out bogus reports, it will be picked up by neighboring IDSs. Large disparities in trust reports can be spotted by the IDS monitoring, and the false reports should be shared with 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 nodesevaluated trust ($0 \leq T_o \leq 1$) for MANETs is proposed in [69]. The node x's trust on node y is given by

$$T_{x,y} = \alpha T_s + \beta T_o \quad (9)$$

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 wronglyinjected 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:

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.

Simple Average of Weighted Products: Average of weighted trust evaluation by all other nodes on y is selected as T_o.

Weighted Average: Weighted average of weighted trust evaluation by all nodes on target node y is selected as T_o.

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

$$T_a(b) = (1-\alpha)Q_a(b) + \alpha R_a(b),\ \ 0 \le \alpha \le 1,\ \ 0 \le Q_a(b) \le 1,\ \ 0 \le R_a(b) \le 1 \qquad (10)$$

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

$$Q_a(b) = \beta E_a(b) + (1-\beta)T_a(b),\ \ 0 \le \beta \le 1 \qquad (11)$$

where $E_a(b)$ represents the trust value obtained by the judgment of the actions of b and $T_a(b)$ gives thelast 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 thecombination 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

$$T_j^i(t+1) = \alpha \times DT_j^i(t) + (1-\alpha) \times RT_j^i(t),\ \ 0 \le \alpha \le 1 \qquad (12)$$

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 "$task$" inthe point of view of x. Now, the trust value on y measured by x with respect to "$task$" is given by

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

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 proposedin [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 employedto 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,

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

where α is the normalized weight factor for the collective evaluation and β is the community context factor.
In [81], a TON-inspired hybrid system for assessing trustworthiness in P2P networks is presented. The TON uses the strength of a link to symbolize the degree to which two peers trust one another. The out-degree of a peer node represents the total amount of comments a user has made on other nodes. An individual's in-degree on a network of peers indicates the total number of recommendations they have gotten. From the ToN's local trust value comes the global reputation values through a Markov chain at random.
In [82], we propose a reputation method for P2P networks based on polling among peers. Using this method of distributed polling, resource requesters can determine whether or not a given resource is reliable. The peer-to-peer trust paradigm relies on both personal "experience" and the "recommendation" of others.
The advantages, disadvantages, complexity, and performance restrictions of several distributed trust computing techniques are compared and contrasted in Table I.

Distributed trust establishment is difficult due to factors such as a lack of established trust infrastructure, scarce resources, temporary connectivity, a shared wireless medium, and physical vulnerability. Some solutions proposed in the literature aim to address these issues by assuming the existence of a central trust authority or trust agent in ad hoc networks. Some methods of establishing trust through trust agents will be discussed below.

B. Establishing Trust Centrally

Most research towards establishing trust centrally relies on the existence of a Trust Agent (TA) that is reachable by every member of the network (see Fig. 4). Here, the TA either determines the community-wide trust value or aids the nodes in determining the trust value by supplying the starting values on target nodes. Depending on how large the network is, there may be just one TA or several.
In [84], the authors suggest a trust computation that is based on the leadership node in a cluster. First, the cluster head distributes to all nodes in the cluster an initial trust value for each other node. When a node combines 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].

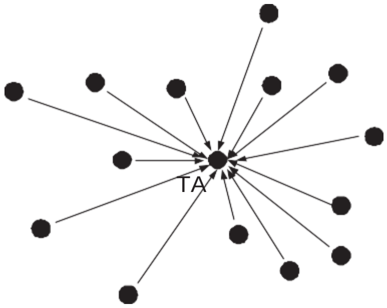


Figure 4. Pictorial representation of the TA based centralized trust computation methods

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 ($\varphi(i,j)$) as follows:

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

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.

A. 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].

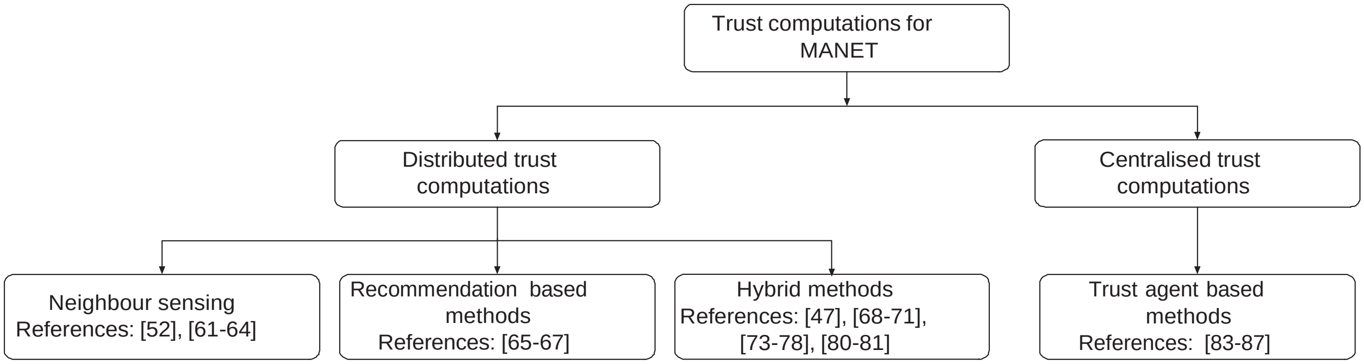

Trust computations for MANET
Distributed trust computations
Centralised trust computations
Neighbour sensing References: [52], [61-64]
Recommendation based methods References: [65-67]
Hybrid methods References: [47], [68-71], [73-78], [80-81]
Trust agent based methods References: [83-87]

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	C	C	C	C	×	×	C	×
Recommendation based methods	×	×	C	C	×	×	×	C
Hybrid methods	×	C	C	C	×	C	C	C
Centralized trust computations								
Trust agent based method	×	C	C	C	×	C	×	C

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 C *denotes successful handling and × denotes unsuccessful handling.*

III. DYNAMICS OF TRUST

Trust dynamics refers to how trust develops and changes over time. Trust is an evolving concept. Time, experience, and the condition of the many sources on which trust is founded (such as surroundings, mobility, etc.) all influence its evolution. Trust propagation, prediction, and aggregation are three processes that help define the trust dynamics. Here, we take stock of what scholars have discovered about these three foundational trust processes.

A. Trust propagation: If the trust is computed on target by one node and then shared with the rest of the network, the time and energy spent recomputation of trust by other nodes can be decreased. In Fig. 6, for instance, node A can learn the trust value of node X via nodes B and C.

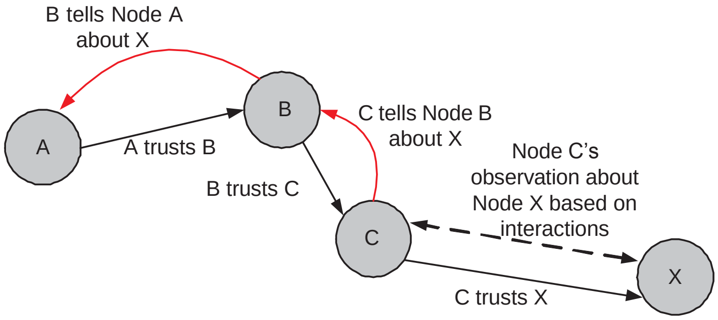


Figure 6. Propagation of trust in a simple straight chain

Don't force Node X to perform an explicit trust calculation. In MANETs, when infrastructure, autonomy, mobility, and resources are all lacking, this is especially crucial. In its simplest form, trust spreads by word-of-mouth, or recommendations. Most people's first line of referral is their next-door neighbor. However, trust may spread in several hops. The trust transitivity feature is the foundation of trust's ability to spread. Cooperation in the network in transmitting the trust information is the essential component in trust propagation. The majority of nodes, if not all of them, must work together to propagate the trust data.

In [103], the notion of a web of trusted nodes that rate unknown nodes is offered as a trust propagation technique for mobile networks. People may tell whether or not they can trust a source of information from which they have never gotten material before based on this web of trust opinion values (this is called "propagating trust" in the technical sense). Based on these assessments, individuals determine whether or not to accept the material. The basic concept is that just a small portion of the web of trust is stored on each mobile device. It then uses a machine learning approach for trust diffusion on that subset.

In [104], the authors offer a method for trust dissemination in mobile wireless networks based on the small world principle. In this case, a transitive network that is limited to a tiny universe propagates trustworthiness. Therefore, it generally only takes a few hops for a node to reach an authenticating node. The other nodes in the path to the authenticating node will use this information to determine how much trust to put in this node. In addition, a transitivity graph-based trust spread is presented in [105].

In [106], the author proposes leveraging one's immediate social circle to spread trust. Here, it was anticipated that node a would spread its confidence in node b to its set S of immediate neighbors. That is, it is expected that trust spreads equally to all immediate neighbors. It is now assumed that all nodes in set S with a one-hop neighbor in node b have a trust level of d. As long as confidence remains over a certain level, this pattern will persist.

In [107], a trust propagation strategy based on Distributed Hash Table (DHT) is investigated for use in a highly mobile overlay network. DHTs leverage ideas like Chord, Pastry to store the trust information and enable the retrieval of data in a dispersed and mobile network. Using a hashing algorithm, these DHTs will automatically simplify and adapt the network's underlying logic. Trust information is disseminated across the network, and the retrieval procedure has a complexity of at most log(N), where N is the total number of nodes. The work in question follows the hash table rule of propagating original evidence as trust information.

In [108], we examine how mobility might be used to spread trust and security credentials. Among the possible policies are: Friend nodes, for instance, can act as authority devices by transporting and relaying trust data. Users have the ability to instantly recognize one another upon first meeting. The choice to establish a trusting connection between two nodes is grounded in this actual meeting. Supporting the process of trust information transfer between geographically adjacent

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.

Don't have Node X calculate trust explicitly if you can help it. This is especially important in MANETs due to the lack of infrastructure, autonomy, mobility, and resources. Trust, in its most elementary form, is contagious through personal recommendations. A person's immediate neighbor is often their first source of recommendation. But trust could spread via a series of intermediary steps. The capacity of trust to spread depends on its transitivity property. The key ingredient in trust propagation is network cooperation in spreading the trust information. In order for the trust information to spread, it is necessary for the vast majority of nodes to cooperate.

As a means of spreading trust in mobile networks, the concept of a web of trusted nodes that rate unknown nodes is presented in [103]. This network of trust opinion values may be used to determine whether or not a new source of information can be trusted (this is technically known as "propagating trust"). It is on the basis of these evaluations that individuals choose to accept or reject the content. The idea is that just a minimal subset of the whole web of trust is kept locally on any one mobile device. On such subset, it employs a machine learning technique for trust diffusion.

The authors of provide a small-world-based approach to trust propagation in mobile wireless networks in [104]. In this situation, credibility is disseminated via a localized transitive network. As a result, the average distance between two nodes is rather small. This data will be used by other nodes along the way to the authenticating node to judge how much faith to place in it. In addition, in [105], a trust spread that relies on transitivity graphs is introduced.

In [106], the writer suggests using one's immediate network to propagate trust. In this case, it was expected that node a's trust in node b would expand to its set S of nearby nodes. That is, trust should naturally extend to include all nearby acquaintances. All nodes in set S that have node b as a direct neighbor are now presumed to have trust level d. This trend will continue so long as optimism is high enough.

The usage of a Distributed Hash Table (DHT) based trust propagation mechanism in a highly mobile overlay network is explored in [107]. Distributed hash tables (DHTs) use concepts like Chord and Pastry to record trust information and facilitate data retrieval in a decentralized and mobile setting. These DHTs will automatically streamline and adjust the network's core logic using a hashing technique. The complexity of the retrieval operation is at most log(N), where N is the total number of nodes, because trust information is broadcast across the network. The relevant work uses the hash table rule, which states that original evidence must be sent down as trust information.

In [108], we investigate the potential of mobile devices to disseminate security credentials and foster a culture of trust. Policy options include the following: For instance, friend nodes can play the role of authoritative devices by carrying and relaying trust information. Users are able to identify one another immediately upon meeting for the first time. The decision to form a reliable link between two nodes is based on this face-to-face encounter. Facilitating the sharing of reliable information between neighboring communities

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 ⊕ should lie in $[0, 1]$. Now, the important conditions for aggregation operator ⊕ 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 $Z(r, s) = \ (B(r, s), D(r, s), U(r, s)$ where

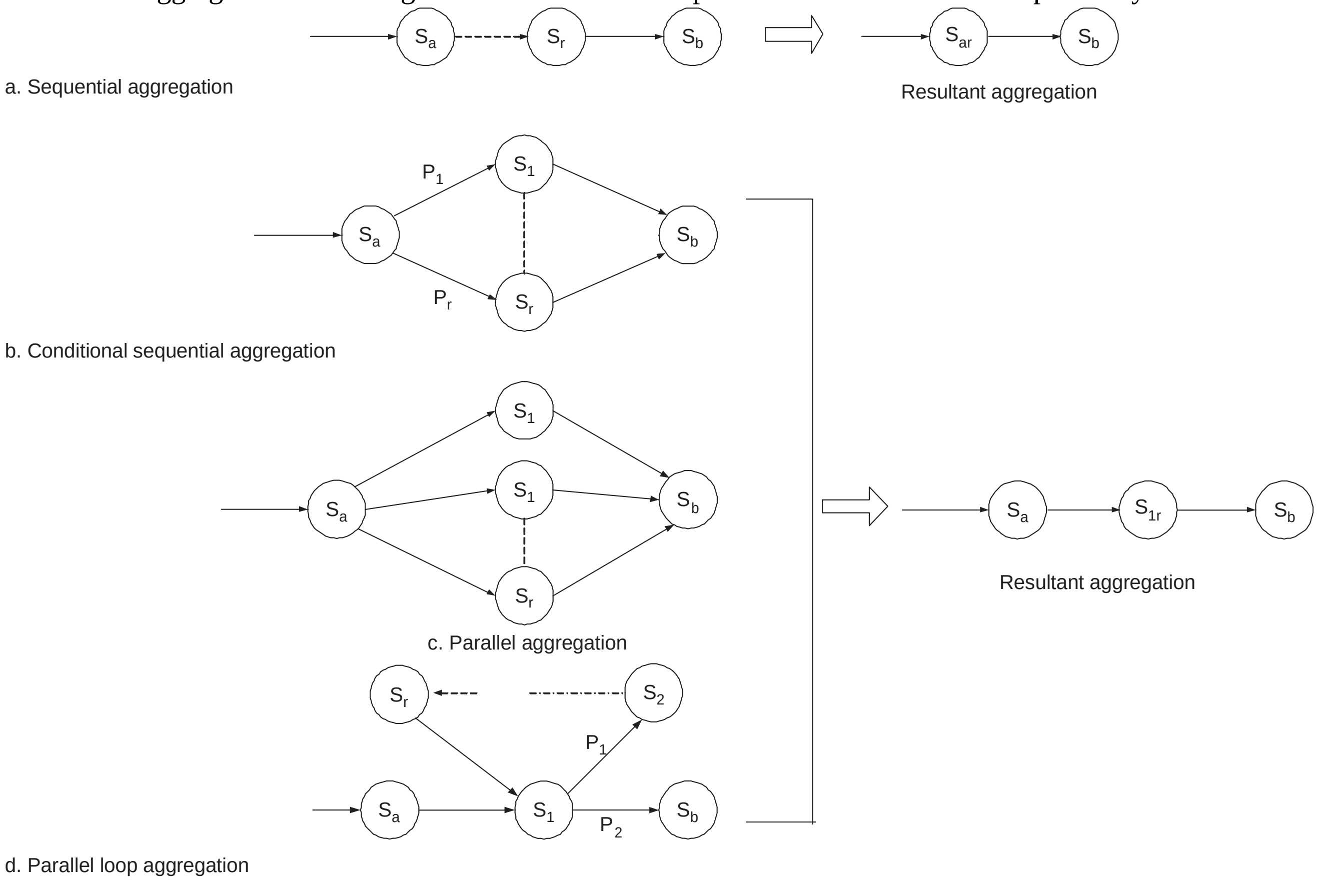
$$B(r, s) = \alpha \frac{r+1}{r+s+2},\ D(r, s) = \alpha\frac{s+1}{r+s+2},\ U(r, s) = 1 - \alpha \tag{22}$$

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



a. Sequential aggregation

Resultant aggregation

b. Conditional sequential aggregation

c. Parallel aggregation

Resultant aggregation

d. Parallel loop aggregation

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 ⊗ is a sequence operator. Now the sequence aggregation of Fig 7. a works as follows

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

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

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

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

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

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

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

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

A. *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.

Kalman filter-based methods are proposed in [123]. Here, the feedback system in Kalman filter averages the reputation values obtained from various nodes. Moreover, the prediction variance is generated using the Kalman filter. Using this dispersion, we may foretell the target node's standing in the network.

Based on the ideas of trust mirroring and trust teleportation, [124] proposes an algorithm for trust prediction. Similarities in people's backgrounds, passions, and skill sets are all taken into account when determining their propensity to trust one another in a trust mirroring exercise. If node a sees that node b shares its interests and its perspective on events based on their prior interactions, then node an is more likely to trust node b's future actions. If node a trusts node b, then any other node with the same set of interests and capabilities as b has a chance of being trusted by an in the future (this is called "trust teleportation").

In [125], we offer a trust prediction system that employs Resnick's prediction formula. An integral component of the trust forecasts is the partner's track record of providing useful advice. That is, if a node has a high rate of correct predictions, it can be considered more reliable than a node with a low rate of correct predictions.

The paper [126] proposes a mathematical induction-based trust prediction model. The authors provide methods for modeling trust variations, which are ultimately applied to the task of estimating the value of trust. Two approaches have been offered. The first tactic is to create a mathematical model of trust fluctuations, which will help to codify trust's historical and prospective dependencies. The second approach involves using a mathematical function that links the current trust representation with the current experience to predict the future trust representation in order to formally model the fluctuations of trust in an inductive manner.

To estimate node reputation from their intrinsic qualities rather than their observable behavior, [127] employs a Radial Basis Function-Neural Network (RBF-NN). In this case, the nodes are identified by a predetermined set of criteria. The starting value of the target's parameter is believed to be known by every node.

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.

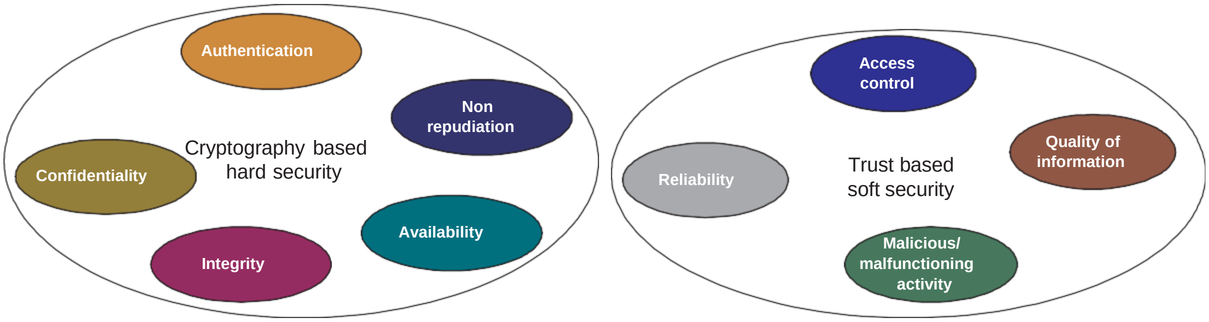
Summary:

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.

IV. 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

offer a measure of protection by facilitating measures like data encryption, node authentication, and non-repudiation. Figure 8 depicts the physical safeguards. Nodes either succeed or fail the security check in a hard security system. In the early stages of a collaborative group, certain nodes may act as legitimate participants, and therefore pass the standard cryptographic security tests. However, they may turn out to be egocentric participants who report inaccurate data, either intentionally or because of malfunctioning hardware. Since these behaviors are always evolving, no rigid security system will be able to help you identify or avoid them. A simple yes/no answer will not work. Hard security also isn't able to adequately analyze the quality of information, provide varying degrees of access control, or ensure the reliability/trustworthiness of data received from nodes. Soft security refers to the group of threats that arise only from the actions of individual nodes [16], [75]. Figure 8 depicts examples of soft security mechanisms. b. Trust management systems are the most effective way to deal with soft security issues [17], [129]. Instead of viewing trust management as a replacement for encryption, consider it an additional layer of security. Together, cryptography and trust management offer a complete security solution for MANET. Here, we take a look at the research done on the topic of trust-based approaches to soft security services such malicious node detection, information quality evaluation, and node trustworthiness. While trust mechanisms may be utilized to boost the efficacy of cryptography-based hard security [130], [133], we don't bother with them here since cryptography necessitates an infrastructure for key management, which is difficult to implement in MANETs.

.

Trust and soft security:

For wireless ad hoc networks, [134] proposes a malicious node detection approach based on trust calculations. In this method, people report suspicious behavior from neighbors to a trusted authority, which then investigates the claims. A global reputation vector is constructed by combining the trust authority's own observations of malicious nodes with the reports of complaints it has received from verified devices. The agent will then send this vector to every node in the network. To determine a device's trustworthiness, authenticated nodes combine their own local trust vector with the global trust vector they get from the trust agent. When this trust level falls below a certain threshold, malicious nodes will be identified.

In [135], we present safe MANET Routing with Trust Intrigue (SMRTI), a trust-based misbehavior detection and safe routing paradigm. The method of hybrid trust assessment used here is similar to that described in [134]. Using the trust prediction approach, SMRTI determines whether or not to send the packet on to the next node. An analogous study of bad actors

There is a proposal for node discovery using trust assessments in [136].

Trust in networks and data security have been the subject of extensive research and development. Inevitably, the trustworthiness of information must be evaluated in relation to the trust level of nodes. Information trust and node level trust may be evaluated, it is assumed, if their respective histories, including origin and specifics of the nodes that processed it (provenance details), are known. In this part, we present some current research on the evaluation of information trust based on its provenance.

In [137], we see an agent-based method for handling the veracity of data in a fluid setting for information exchange. Information objects, made up of metadata and data, are used to store and retrieve information in this framework. Information about where information came from (its "provenance") is one of the qualities defined by meta data. It is possible to ascertain whether or not two trust evaluations are independent by constructing a provenance graph for a derived information item using meta data. The credibility of data items is then assessed using the Dempster-Shafer theory.

Another data provenance trust model is provided in [138] that uses trust scores to determine the credibility of both data and data providers. Data similarity, data path similarity, data conflict, and data deduction are only few of the considerations made to ensure that the data is as trustworthy as possible. If a node consistently offers accurate information, then the information it provides is more likely to be true. An iterative approach for calculating information trustworthiness is proposed on the basis of such interdependencies.

In [83], the authors suggest a method for evaluating the reliability of data based on how similar its components are. The concept is that if two pieces of information arrive at the same destination via different channels but have comparable contents, then both the information and the nodes involved in its processing are likely reliable. Using the receiver's assessment of the reliability of the information, a feedback mechanism is offered to dynamically modify the nodes' trust values.

Collusion attacks [139] can be used to compromise the trustworthiness evaluation methodology given in [138]. In [139], a majority rule based approach is presented for identifying malevolent cooperating parties. Clusters of data points C0,..., Ci are supposed to constitute the evidences for an event E. Ck is believed to have true information and the other clusters to contain false information if and only if the average trust score of Ck (0 k i) is greater than the average trust score of any other cluster. Penalty functions are proposed to lower the trust scores of nodes that produced the colluding evidence items based on this finding.

In [140], we are made aware of a few research gaps in the area of provenance-based information trust analysis.

V. CONCLUSION AND FUTURE WORK

Research on the cultivation and maintenance of trust is fascinating. The rapidly expanding body of literature on the topic of trust provides compelling evidence that this is a vital topic for study. Different approaches to trust management have arisen because the notion of trust may be used in many different contexts. The purpose of this article is to help MANETs' designers gain an appreciation for trust from many angles, learn what characteristics should be included in a trust metric, and gain insight into how trust might be calculated. At the outset of this work, we introduced many distinct trust definitions and measures. Then, we compared and contrasted the various trust computing methods with regard to the aforementioned attack models and computational burdens. We combed through the literature on trust dynamics, taking into account topics like trust's ability to spread, aggregate, and be predicted. We conclude with a discussion on how trust mechanisms might be used to enhance safety.

There is a vast variety of processes at work in the many trust systems given in this research. There is no silver bullet that can be applied universally, and applications. It is important to think about the limitations of the network and the kinds of information it can accept while creating a new trust system. It has been noted that the current body of research and suggestions is incomplete. There are still significant problems to solve. Here are just a few examples:

Trust and the role of network dynamics: While we have provided a high-level overview of how network dynamics affect the various trust dynamics, further investigation is required. For instance, trust amplification and other security paradigms may be affected by mobility. But the precise quantitative connection has yet to be established. It remains to be investigated how other aspects of networks (such as link dynamics and network density) relate to trust and its evolution.

- Trust computations in cooperative and noncooperative games: in a decentralized network, nodes may suggest others either positively or negatively, either out of genuine concern or out of malice motivated by personal gain. These features are similar to those seen in complex systems that involve interactions based on game theory [141]. Non-cooperative games have each node compete against the others, whereas cooperative games have groups of nodes work together to take on the entire network [142]. Nash equilibrium makes it possible to solve non-cooperative games [143]. The analysis of trust computation in a cooperative game is still in its early stages. Preliminary attempts leverage beneficial collaborations to derive trust scores [142], but these efforts are still in their infancy.
- The effect of diverse nodes on confidence: It's possible that wireless networks will be quite diverse. The nodes' responsibilities, capabilities, and even safety might all contribute to the aforementioned diversity. Due to heterogeneity, not all nodes or their contents may be given the same weight for determining credibility. As a result, not all nodes' trustworthiness will be assessed using the same functional descriptions. The integration of network dynamics and heterogeneity into trust evaluation functions requires further study.
- Security principles that improve online confidence: A user's confidence in the data they get is strongly related to the network's data delivery capabilities and security features. For instance, unless both the information's origin and its transmission channel are

verified, it may be unreliable. One must select whether to have the untrusted information or none at all if authentication services are unavailable. More study is needed to define and characterize these metrics so that we may learn how much security features affect network trust.

Trust in social relationships and the context in which such relationships exist has attracted a lot of study in recent years [144]. However, in terms of MANET, this is still a mostly uncharted territory. However, MANET has yet to investigate the intricate interdependence of these three networks: communication, social, and application. Validating trust metrics also need input from social communities. Another important topic for further study is the verification of trust measurements.

Consolidation around a set of core principles for creating trust and its numerous linked concerns, with practical and commercial applications achieved, is something we want to see in the near future.

REFERENCES

[1] "Using trust for secure collaboration in uncertain environments," by V. Cahill et al., published in IEEE Pervasive Computing, volume 2(3), pages 52-61, 2003.

[2] "Trusting Collaboration in Global Computing Systems," Lecture Notes in Computer Science, Springer-Verlag, vol. 2692, pp. 136-149, 2003. Authors: C. English, W. Wagealla, P. Nixon, S. Terzis, H. Lowe, and A. McGettrick.

"Cooperation and trust: Some theoretical notes," by M. Deutch (pp. 275-319 in the 1962 edition of Nebraska Symposium on Motivation published by Nebraska University Press).

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

"Trust-based security for wireless ad hoc and sensor networks," by A. Boukerch, L. Xu, and K. EL-Khatib, published in Computer Communications, vol. 30, pages 2413-2427, 2007.

According to

[4] "Trust-based security in pervasive computing environments," published in IEEE Computer, volume 34, pages 154-157, 2001. Authors L. Kagal, T. Finin, and A. Joshi.

"Distributed resources in wireless networks: Discovery and cooperative uses," by H. Sarvanko, M. Hyhty, M. Katz, and F. Fitzek, published in the proceedings of the 4th ERCIM eMobility Workshop held in conjunction with WWIC 2010.

Based on the work of M. A. Ayachi, C. Bidan, T. Abbes, and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol," International Symposium on Trusted Computing and Communications, Trustcom, 2009, pp. 802-808.

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

For example, see

[5] "Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs," published in IEEE Trans. Veh. Technol., vol. 58, no. 4, May 2009.

"A survey on distributed approaches to graph based reputation measures," by K. Avrachenkov, D. Nemirovsky, and K. S. Pham, was published in 2007 in the proceedings of the second international conference on performance assessment techniques and tools.

M. Momani, "Trust models in wireless sensor networks: A survey," Recent Trends in Network Security and Applications, volume 89, issue 1, pages 37-46, Communications in Computer and Information Science, 2010.

"Trust management survey," by S. Ruohomaa and L. Kutvonen, was published in 2005 as part of the Itrust conference's lecture notes on computer science (notebook reference: 3477).

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

"A survey on trust and reputation schemes in ad hoc networks," by M. A. Azer, S. M. El-Kassas, A. W. F. Hassan, and M. S. El-Soudani, was published in 2008 in the proceedings of the Third International Conference on Availability, Reliability, and Security (ARES 08), pages 881-886.

Referring to the work of A. Jsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst., volume 43, issue 2, pages 618-644, 2007.

[6] "A survey of trust and reputation management systems in wireless communications," H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato published in Proc. IEEE, volume 98, issue 10, pages 1752–1754, October 2010.

"A survey of trust in internet applications," by T. Grandison and M. Sloman, published in IEEE Communications Tutorials, volume 3, pages 2-16, 2000.

[7] "A survey of secure mobile ad hoc routing protocols," published in IEEE Commun. Surveys Tuts., volume 10, issue 4, pages 78-93 in 2008.

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

As cited in

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

According to

[9] "Trust-based fast authentication for multiowner wireless networks," IEEE Trans. Mobile Comput., vol. 7, no. 2, pp. 247-261, 2008.

"On trust evaluation in mobile ad hoc networks," [23] D. Q. Nguyen, L. Lamont, and P. C. Mason. Privacy and data protection in wireless networks and mobile devices, 2009 Springer, pp. 1-13 in volume 17.

Trust as a social reality," by J. D. Lewis and A. J. Weigert (24). Trust, Social Atomism, and Holism, all from the book "Social Forces." 1985, volume 63, issue 4 of The Sociological Quarterly, pages 967–985.

As cited in

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

[11] J. B. Rotter, "A new scale for the measurement of interpersonal trust," Journal of Personality, vol. 35, no. 4, 1967, pp. 651-665.

"Trust and the appraisal process in close relationships,"
[12] J. G. Holmes. Advances in personal relationships, volume 2, edited by W. H. Jones and D. Perlman, 1991, pages 57-104.
For example, see
[13] O. E. Williamson, "Calculativeness, trust, and economic organization," Journal of Law and Economics, vol. 34, pp. 453-502 (1993).
As cited in
[14] P. Sztompka, "Trust: A Sociological Theory," Cambridge: Cambridge University Press, 1999.

[15] "An integrative model of organizational trust," by R. C. Mayer, J. H. Davis, and F. D. Schoorman, published in the Academy of Management Review, volume 20, pages 709-734, 1995.
[16] D. J. McAllister, "Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations," Academy of Management Journal, vol. 38, issue 1, pp. 24-59, 1995.
[17] L. Ding, P. Kolari, S. Ganjugunte, T. Finin, A. Joshi, "Modeling and evaluating trust network inference," Workshop on Deception, Fraud, and Trust in Agent Societies, Third International Joint Conference on Autonomous Agents and Multi-Agent Systems, AAMAS'04, pp. 21-32, July, 2004.
[18] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in New security paradigms: proceedings of the ACM workshop, pp. 48–60, 1998.
Based on the work of G. Elofson, "Developing trust with intelligent agents: An exploratory study," published in 1998's The First International Workshop on Trust, pages 125-139.
"A fuzzy approach to a belief-based trust computation," by R. Falcone, G. Pezzulo, and C. Castelfranchi, was published in 2003 as part of the Lecture Notes Artificial Intelligence.
"Trust is much more than subjective probability: Mental components and sources of trust," by C. Castelfranchi and R. Falcone, published in 2000's Proceedings of the 33rd Hawaii International Conference on System Sciences.
According to
[19] "Security and trust issues in semantic grids," written by D. Olmedilla, O. Rana, B. Matthews, and W. Nejdl, and published in Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies, vol. 05271, 2005.
Specifically,
[20] D. Gambetta, "Can we trust trust?," Trust: The Building and Destruction of Relationships of Cooperation Edited by David Gambetta. Pages 213–237 in Basil Blackwell's 1990 Oxford publication.
From Springer-Verlag: "Exploring different types of trust propagation," Lecture notes in computer science, volume 39, issue 1, pages 179–192, 2006.
[21] "Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation," ACM Transactions on Information System Security, volume 6(1), pages 1-42, 2003. Authors: T. Yu, M. Winslett, K. E. Seamons.
"A computational model of trust and reputation," by L. Mui, M. Mohtashemi, and A. Halberstadt; published in 2002 as part of the proceedings of the 35th Hawaii International Conference on System Science (HICSS'02).
For a comparison of several trust computation methods, see
[22] G. Theodorakopoulos and J. S. Baras, "A testbed for comparing trust computation algorithms." http://infoscience.epfl.ch/record/111326/files/gtjb-asc06a.pdf.
"Valuation of trust in open networks," by T. Beth, M. Borcherding, and B. Klein, was published in 1994 as part of Volume 875 of Lecture Notes in Computer Science.
[23] "Eigenrep: Reputation management in P2P networks," by S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina in World- Wide Web Conference, 2003.
[45] "Cooperative peer groups in NICE," Comput. Netw., vol. 50, no. 4, pp. 523- 544, 2006.
According to
[24] "Modeling and managing the trust for wireless and mobile ad-hoc networks," written by Y. Ren and A. Boukerche and published in IEEE's International Conference on Communications (ICC) 2008, pages 2129-2133.
For example, see
[25] 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.
Theodorakopoulos, G., and Baras, J. S. "Trust evaluation in ad-hoc networks," in Proceedings of the Third Annual ACM Workshop on Wireless Security (WiSe 2004), pp. 1-10, 2004.
A. Jsang, "An algebra for assessing trust in certification chains," in Proceedings of the 1999 Network and Distributed Systems Security Symposium, NDSS 99.
"Trust-enhanced security in location-based adaptive authentication," by G. Lenzini, M. S. Bargh, and B. Hulsebosch, was published in 2008 in Electronic Notes in Theoretical Computer Science, volume 197, issue 1, pages 105-119.

[26] R. Haenni, "Using probabilistic argumentation for key validation in public-key cryptography," International Journal of Approximate Reasoning, vol. 38(3), 2005, pp. 355-376.
"Statistical trust establishment in wireless sensor networks," by M. J. Probst and S. K. Kasera, was published in 2007 as part of the proceedings for the 13th International Conference on Parallel and Distributed Systems.
[27] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust cooperative trust establishment for MANETs," in The fourth ACM symposium on security of ad hoc and sensor networks, pp. 23-34, 2006.
[54] "The beta reputation system," by A. Jsang and R. Ismail, published in Proc. BCEC, pp. 324-337, 2002.
[28] "Research on a fuzzy logic-based subjective trust management model," T. Wen, H. Jianbin, and C. Zhong published in the Journal of Computer Research and Development vol. 42(10), pages 1654-1659, 2005.
The following is a direct quote from "A trust model based on fuzzy recommendation for mobile ad-hoc networks," written by J. Luo, X. Liu, and M. Fan and published in Comput. Netw., volume 53, issue 14, pages 2396-2407 in 2009.
V. S. Grishchenko, "A Fuzzy Model for Context-Dependent Reputation," Trust, Security, and Reputation Workshop Proceedings, International Society for Web Conferences, 2004.
"Fuzzy trust for Peer-to-Peer based systems," by F. Azzedin, A. Ridha, and A. Rizvi, World Academy of Science, Engineering, and Technology, 2007, pp. 123-127.