A Multidimensional Trust Evaluation Model for MANETs

Antesar M. Shabut[a], M Shamim Kaiser[b], Keshav P. Dahal[c,d], Wenbing Chen[d]

[a]*Anglia Ruskin IT Institute, Anglia Ruskin University (ARU), Chelmsford, UK*
[b]*Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh*
[c]*School of Engineering and Computing, University of the West of Scotland, Scotland, UK*
[d]*School of Mathematics and Statistics, Nanjing University of Information Science and Technology, China*

Abstract

Effective trust management can enhance nodes' cooperation in selecting trustworthy and optimal paths between the source and destination nodes in mobile ad hoc networks (MANETs). It allows the wireless nodes (WNs) in a MANET environment to deal with uncertainty about the future actions of other participants. The main challenges in MANETs are time-varying network architecture due to the mobility of WNs, the presence of attack-prone nodes, and extreme resource limitations. In this paper, an energy-aware and social trust inspired multidimensional trust management model is proposed to achieve enhanced quality of service (QoS) parameters by overcoming these challenges. The trust management model calculates the trust value of the WNs through peer to peer and link evaluations. Energy and social trust are utilized for peer to peer evaluation, while an optimal routing path with a small number of intermediate nodes with minimum acceptable trust value is used for evaluation of the link. Empirical analysis reveals that the proposed trust model is robust and accurate in comparison to the state-of-the-art model for MANETs.

Keywords:
Trust management model, social properties, recommendation management, peer to peer evaluation, link evaluation

---

1. Introduction

A mobile ad hoc network or MANET comprises autonomous wireless nodes (WNs) communicating with one another without the assistance of access-points or backbone infrastructures. These WNs act as intermediate nodes, configure dynamically and cooperate with each other to forward data transmissions from the source through a pre-selected routing path to the destination [1, 2, 3]. MANETs are widely employed for military operations, personal area network applications and emergency rescue operations [4]. Such wireless networks are time-varying due to the frequent mobility of the WNs. Thus, link failure, network security and quality of service (QoS) are open challenges for researchers [5, 6, 7, 8].

Existing methods for securing routing protocols in MANETs may not be appropriate or may compromise QoS. Many of these approaches propose cryptography models to secure MANETs. However, such models are irrational, as the authors have assumed that all the WNs in MANETs are trustworthy, and those models may allow for a very simple denial of service (DoS) attack[9]. To mitigate these limitations and also improve the overall performance of the routing protocols, researchers have used the social concept of trust management to secure WNs. Trust models in MANETs [10, 11, 12, 13] monitor the cooperation of WNs through packet forwarding to evaluate the trustworthiness of WNs. However, only monitoring node cooperation cannot represent the complexity and subjectivity of trust metrics [14, 15, 16]. While this approach can be used to find routes with a certain degree of confidence, it may not secure WNs from various types of network attacks. In addition, it omits the consideration of dynamic characteristics of MANETs and does not offer the opportunity to collect multi-source information [12, 17]. Including multiple trust attributes of WNs from social network analysis [18] such as friendship, honesty, level of cooperation, reputation and community of interest relationships to establish and manage trust in a distributed fashion can enhance monitoring of the behaviour and cooperation of WNs and consequently, improve evaluations of trustworthiness [19, 13]. Therefore, multidimensional factors such as social information and QoS should be considered when managing trust-based routing in MANETs.

Trust in distributed systems has been introduced as the degree of subjective belief in a particular node's behaviour [20]. Thus, similar to human behaviour, a node, called the *evaluating node*, assesses the behaviour of another node, called the *evaluated node* based on the level of trust derived from direct experiences or historical interactions between the two nodes in MANETs. The other nodes in a society can also recommend evaluated nodes based on past interactions, and these nodes are called *recommending nodes*. The trust value evaluated through this human behaviour process is random, and rises and decays over time. Thus, the behaviour of WNs in MANETs is similar to the human behaviour model, where some nodes have never previously interacted with certain other nodes, and these nodes become acquainted with each other for interaction with other nodes based on a certain trust level which has developed over time [21]. However, the interactions of these nodes exhibit different types of misbehaviour, which include selfishness by avoiding participation in routing activities when taking into consideration limitations in certain resources such as energy, and dishonesty in assessing or providing trust information [20]. These types of misbehaviour can break the basic functionality of the MANET system.

This paper presents a trust management framework with a multidimensional trust metric, considering social and QoS properties to mitigate misbehaviour of WNs in MANETs. Social properties include the frequency of interactions, honesty and closeness centrality, while QoS properties include nodes energy consumption. The paper also measures the effect of social properties on the routing performance of the network. Trust evaluation is conducted in two ways; peer to peer and link evaluation. In peer-to-peer evaluation, the trust value of two nodes is evaluated by considering social parameters and nodes' energy when they interact during packet forwarding activities. On the other hand, link evaluation assesses the selection of a trustworthy path among different available paths. The main contribution of this work is outlined below:

- Firstly, the proposed framework utilises a multidimensional trust metric considering social properties and nodes' energy, and then evaluates the trust relationship among nodes. As the trustworthiness of the network is increased through this trust framework, overall network efficiency will improve.

- Secondly, peer-to-peer evaluation and link evaluation are employed to evaluate the trustworthiness of the WNs in the network. In peer-to-peer evaluation, the trustworthiness of neighbour nodes is evaluated to determine whether to interact with them or not, which is based on social and QoS properties. Link evaluation selects a trustworthy path from a source node to a destination node based on an optimal trust combination, where each intermediate node on the path has a minimum acceptable trust value. This two-stage evaluation can enhance the accuracy of the model and have a positive impact on improving network performance.

The rest of the work is ordered as follows. Section 2 discusses related works; Section 3 illustrates a scenario where the trust model evaluates the trust values of WNs of a MANET; Section 4 provides a detailed discussion of various trust factors which are considered in evaluating the trust value of a WN; Section 5 presents the simulation results; and finally, conclusions and suggestions for future directions for improvement are provided in Section 6.

2. Related Works

Trust and reputation management plays an important role in the successful achievement of transactions between nodes in MANETs, where cooperation is essential to perform network activities.

Recently, researchers have noted the significance of using the trust management concept from social networks in building and analysing trust relationships among nodes [22]. Trust and reputation models would promote confidence in the integrity of MANETs services and reinforce the benefits of this technological revolution.

Over recent years, several trust and reputation models have been proposed to enhance security in MANETs, with the aim of empowering nodes to assess their neighbours' behaviours directly or through recommendations from other nodes in the network [12, 23, 24, 16, 24, 25, 26]. However, most existing trust models quantify and predict trustworthiness among nodes based on a simple or single trust evaluation metric. This single measure may not be capable of satisfactorily assessing the trustworthiness of nodes in many scenarios of dynamic MANETs [27, 28, 26]. A multidimensional trust evaluation method that considers different network requirements and social properties of trust to quantify and predict nodes trustworthiness is still a challenging problem for MANETs. Absence of considering the quality of communication, selfishness behaviours, malicious intent, the absence of fixed infrastructure, limited resources and physical failures can mean that resulting trustworthiness scores are extremely inflated and noisy, which makes it difficult for nodes to find a trustworthy partner to achieve the required task.

In [23] the authors propose a trust-based reputation system to evaluate the trustworthiness of nodes in MANETs. Only a single trust metric is used to evaluate the trustworthiness of nodes, based on the cooperation of nodes in packet forwarding. The model, therefore, omits some important evaluation metrics, including energy, delay and social properties in evaluating nodes trustworthiness. Meanwhile, [16] propose TRUNCMAN, which is a trust-based routing model utilized by the authors to isolate non-cooperative nodes during route discovery activities and safeguard the network against many network layer attacks, including black and grey hole attack (dropping packets). The proposed protocol includes two phases: the Suspicion Phase, which checks the activities related to route request broadcast and acknowledgement; and the Detection Phase, which provides details of the detection of non-cooperative nodes. Isolation and propagation of malicious behaviours targeting the attacker nodes in the network is broadcast as social welfare. Similarly, this model also evaluates the nodes trustworthiness only based on packet forwarding, omitting consideration of the dynamic characteristics of MANETs, as well as the quality of paths and social network properties. Our previous work in [12] studied the problem of dishonest recommendation in the presence of attacks related to the recommendation, including bad-mouthing and ballot-stuffing attacks, to develop an effective filtering algorithm of recommendations in MANETs. The model considers some social trust factors to filter out dishonest recommender nodes, and includes: majority opinion by all recommender nodes; the personal experience of the evaluating node; and service reputation, which evaluates the consistency of cooperation in packet forwarding and provides recommendations. Recommendations are clustered, filtered, and selected based on the three factors listed above. However, although the model considers some social attributes, the energy and time-varying properties of WNs are not considered.

Some existing trust models considering multidimensional properties for building trust relationships between nodes in MANETs [29, 30, 27] do not consider social trust relationships between nodes. Yunfang [29] proposes a combination of policy and reputation-based approaches structured into an adaptive trust management framework, thereby addressing the issue of firm/objective security as well as subjective security. However, the basis of this work depends completely on the assumption that trust is transitive, and it is not clear how a more realistic transitivity model can be incorporated into the trust management system.

The authors in [27] propose a multi-dimensional model to evaluate the trustworthiness of nodes in a MANET from multiple perspectives (i.e. dimensions). These dimensions include collaboration trust, behavioural trust, and reference trust derived from multiple sets of misbehaviours and different types of observations. However, network requirements and social trust relationships are not considered when evaluating the trustworthiness of nodes in the network.

Yu et al. also consider the problem of proposing a composite trust metric [31, 32]. They present a trust model with multiple decision factors, in which two types of trust; security trust and quality trust, are incorporated in evaluating the trustworthiness of nodes in MANETs. Analytic Hierarchy Process (AHP) methodology is used to combine these two trust types. This work uses transmitting trust and energy trust to evaluate the security trust of nodes, while it uses delay trust and delay jitter trust to evaluate the quality of trust. Furthermore, social network properties were omitted in evaluating the trustworthiness of nodes in the network.

Authors in [28] propose a light-weight trust-enhanced model for multi-path routing in MANETs. They focus on the concept of a trust inference model, where each node has a trust value for its neighbour, and these form the basic building blocks of this model. Multi-dimensional trust attributes are incorporated to address the complexity of the trust relationships between nodes based on historical experience. These attributes are weighted using fuzzy AHP scheme based on entropy weight measure. The model incurred a small additional overhead in order to provide considerable security measures for the routing protocols in MANETs. In this model, QoS and social attributes were not considered for the calculation of trustworthiness values.

Wang et al. in [32] propose a multidimensional trust-based model to solve the problem of decision making in service composition and binding for service-oriented MANETs. The authors propose two trust dimensions: competence, which refers to a service providers capability to adequately serve the received request; and integrity, which refers to the degree to which a node complies with the prescribed protocol. They conduct extensive simulations to test the performance of their proposed trust model against a non-trust-based scheme and an existing single-trust-based scheme. Their results show that the proposed algorithm can outperform the existing single trust-based model by effectively filtering out malicious nodes conducting various attacks, as well as penalizing attackers with loss of reputation, which may lead to user satisfaction. In addition, their model is efficient, with linear run time complexity, achieving a close-to-optimal solution.

From the discussion above, it is obvious that evaluating trustworthiness based on composite factors, which include network requirements and social trust properties, is still an open and challenging problem. With the proliferation of powerful mobile devices and wireless technology, nodes can provide and receive services, which accelerates the transformation from traditional MANETs to a new era of service-oriented MANETs [32]. However, most of the existing trust models fail to consider social relationships among MANET nodes, as well as the mobility issues which affect these relationships [33]. The above models lack simultaneous consideration of malicious nodes, social behavior, and QoS requirements [34]. For example, selfish behaviour which is considered as non-malicious may lead to packet-dropping due to buffer overflow or expiration of Time-to-Live in the routing protocol. On the other hand, A node which is good socially may misbehave maliciously by providing dishonest recommendations and confusing the trust model. Therefore, it is vital to address the conflict in the nodes' behaviours together with the QoS requirements in the network. Moreover, not considering these factors can make these models unsuitable for service-oriented MANETs. Although some models consider some social ties, there is no clear analysis given on how these social ties could help in improving the trust models accuracy, and the performance of the network. As a result, this may lead to inaccurate quantification and prediction of trustworthiness, and consequently, mislead nodes in the decision-making procedure. To address the aforementioned issues within the current literature, we propose a feasible trust model which, unlike existing trust protocols for MANETs, deals with scalability, heterogeneity, mobility, and social relationships.

3. The Proposed Multidimensional Trust Model

The proposed trust model, along with the MANET architecture, is illustrated in Figure 1. The MANET architecture contains various categories of WNs, as discussed in 3.1, while the trust model incorporates the Bayesian statistical function to evaluate the social trust values of these WNs, as explained in Section 3.2.

3.1. A MANET Architecture

In the proposed scenario, the MANET comprises three types of WNs: these are termed the evaluating node, evaluated node, and recommending node. Figure 1 illustrates a node WN_1 which is evaluating the trustworthiness of a neighbour node WN_2 at time t, while the other k neighbour nodes WN_{k_1}, WN_{k_2}, WN_{k_3}, ... WN_{k_n} also provide a recommendation for WN_2 at the same time t. In this case, WN_1 and WN_2 are called evaluating and evaluated nodes respectively, whereas WN_{k_1}, WN_{k_2}, WN_{k_3}, ... WN_{k_n} are the recommending nodes and n is the number of recommending nodes.

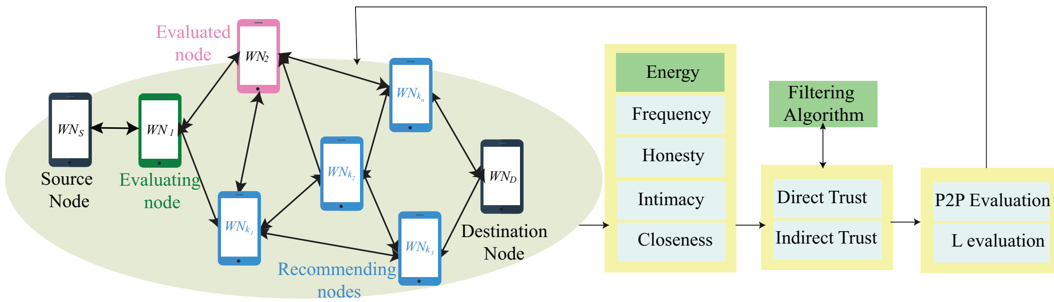


Figure 1: A MANET architecture at time t with the proposed trust model. The trust model computes the trust value of each WN using the social trust component and node energy. A node WN_1 evaluates the trustworthiness of a neighbour node WN_2 at time t (direct trust), and the other neighbour nodes WN_{k_1}, WN_{k_2}, WN_{k_3} ... WN_{k_n} also provide recommendations for the WN_2 at the same time t (indirect trust).

The trustworthiness of a node can be evaluated by summing the direct and indirect trust values. The direct trust value is found using previous direct interactions between the evaluating and evaluated WN, and the indirect trust value is calculated using the trust value suggested by the recommending nodes based on their trustworthiness with the evaluating WN. The direct trust value is accurate and is invulnerable to dishonest recommendation. However, an indirect recommendation can be vulnerable, due to the dishonest recommendations of the other neighbour nodes, and in such recommendations, it is equally important to understand the selfishness/malicious behaviour of WNs in the network. The issue of dishonest recommendation and the cost of the extra messages exchanged by the recommending nodes for the performance and energy of the proposed model, besides the problem of data sparsity, were discussed in [12, 35, 36].

The proposed trust model aims to secure the optimal routing path of a source-destination (S-D) pair using peer to peer (P2P) evaluation and link (L) evaluation. The energy and social trust of WNs are utilized for P2P-evaluation, whereas the optimal routing path, having a lower number of intermediate nodes with minimum acceptable trust value, is used for L-evaluation. In P2P-evaluation, a WN evaluates the numerical score of the behaviour (mainly selfishness and maliciousness) of its neighbour WNs prior to developing a trust relationship. The P2P trust value utilizes direct and indirect trust values, and suggests that the evaluating node selects the next hop or evaluated node to relay/forward the information. Meanwhile, the L trust value is evaluated based on the optimal routing path and trustworthiness of intermediate WNs on the path between the S-D link.

If WN_i and WN_j are evaluating node and evaluated node respectively, using the four trust factors of frequency, intimacy, honesty and energy during the interaction, the trust value $T_{ij}(t)$ of WN_j is assessed by WN_i at time t and the trust value $T_{kj}(t)$ of WN_j is assessed by WN_k at time t and received by WN_i with a weight factor, where $k = 1, 2, 3, ...n$, and n is the number of recommending nodes. Mathematically, the trust value of WN_j assessed by WN_i is calculated by

$$T_{ij}(t) = w_D T_{ij}^D(t) + w_I T_{kj}^I(t) \tag{1}$$

where $T_{ij}^D(t) = w_f T_{ij}^f(t) + w_h T_{ij}^h(t) + w_{int} T_{ij}^{int}(t) + w_e T_{ij}^e(t)$ is calculated via the direct method and $T_{kj}^I(t) = w_f \sum_{k=1}^n T_{kj}^f(t) + w_h \sum_{k=1}^n T_{kj}^h(t) + w_{int} \sum_{k=1}^n T_{kj}^{int}(t) + w_e \sum_{k=1}^n T_{kj}^e(t)$ is calculated via the indirect method, w_D and w_I are the direct and indirect trust weight and $w_D + w_I = 1$, while w_f, w_h, w_{int} and w_e are the weight values for the four factors and $w_f + w_h + w_{int} + w_e = 1$.

3.2. Bayesian Statistical Function

Similar to [37], the proposed trust model employs the Bayesian statistical approach to evaluate social trust value, which obeys beta distribution. Beta distribution and Bayesian inference techniques are utilized in this paper because they represent a less resource-intensive method of evaluating the trustworthiness of a node within two values, α and β, which is simple to store and compute in the MANET system with constrained resources. Moreover, this approach forms a way to evaluate the accumulated number of experiences (i.e. interactions) a node can have during its network activities, and enables the combination of experiences from different sources, including direct experiences and recommendations received from others, because of the addition property of the beta function. Therefore, it reflects the dynamic nature of trust, which is dependent on the accumulated number of experiences, and captures the uncertainty property of trust because the beta function can give only a probabilistic estimation of future trust. Using gamma function, beta distribution $f(p|\alpha, \beta)$ can be defined by equation (2)

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (2)$$

where α and β are the aggregated positive observation when a node forwards packets and the aggregated negative observation when a node drops packets, p is the probability, $p \in [0,1]$ for α, $\beta > 0$; $p \neq 0$ if $\alpha < 1$ and $p \neq 1$ if $\beta < 1$. Consider that the new positive and negative interactions between WN_i and WN_j are evaluated as ρ and σ respectively. Then, after each observation, $\alpha = \rho + 1$ and $\beta = \sigma + 1$ where $\rho, \sigma > 0$. The mean and standard deviation of $f(p|\alpha,\beta)$ can be expressed by equations (3) and (4).

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad (3)$$

$$S(p) = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \quad (4)$$

Let $T_{ij}(t)$ equal the trust value at time t for interactions between WN_i and WN_j, which changes over t in the dynamic environment of the MANET. At the beginning (i.e., $t = 0$) of the trust relationship between these nodes, $\alpha = \beta = 1$ which result in $T_{ij}(0) = 0.5$ calculated by equation (3). For $t > 0$, the WN_i calculates $T_{ij}(t)$ for WN_j by aggregating the positive and negative interactions between these nodes using equations (5) and (6) and then use equation (3) to calculate the trust value.

In order to give higher priority to recent interactions and to reduce the influence of previous interactions over t, we include a decay factor μ. Consider the new positive and negative interactions between WN_i and WN_j as ρ_{new} and σ_{new} respectively between the time interval t_1 and t_2. Thus, ρ and σ after time t_2 can be calculated by equations (5) and (6).

$$\rho = \rho_{new} + \rho\mu \quad (5)$$

$$\sigma = \sigma_{new} + \sigma\mu \quad (6)$$

On the other hand, when there is no new interaction existing between WN_i and WN_j during the time interval $[t_1, t_2]$, ρ and σ after time t_2 can be calculated by $\rho = \rho\mu$ and $\sigma = \sigma\mu$.

4. Evaluation of Trust Factors

4.1. P2P trust factors

The P2P trust factor is evaluated by evaluating WNs. Considering four components of trust, an evaluating WN_i estimates the trustworthiness of an evaluated WN_j. These four trust components are discussed in the following subsections.

4.1.1. Frequency based social trust factor

The frequency based social trust factor refers to the connection between two interacting WNs. The higher the frequency of interaction, the stronger the friendship. Many studies utilise the frequency factor to understand the strength of the routing protocols in MANETs and mobile social networks [38]. The frequency-based social trust factor is estimated by evaluating the number of interactions between both the evaluating and evaluated nodes. A high frequency of interactions indicates that the WN_i and WN_j have a strong relationship. Frequency based social trust evaluation, $T_{ij}^{f}(t)$, can be calculated using the variances of all experiences between nodes. Consider that node WN_i has positive and negative interaction with node WN_j at time t. Using the beta standard deviation (S_{ij}), mathematically, $T_{ij}^{f}(t)$ is expressed using equation 7.

$$T_{ij}^{f}(t) = 1 - \sqrt{12S_{ij}} = 1 - \sqrt{12\frac{\alpha_{ij}\beta_{ij}}{(\alpha_{ij}+\beta_{ij})^2(\alpha_{ij}+\beta_{ij}+1)}} \tag{7}$$

The value of $T_{ij}^{f}(t)$ lies between $[0,1]$. At $t = 0$, $\alpha = \beta = 1$: that is, the interaction between WN_i and WN_j nodes is zero (i.e., the number of interactions $N_{ij} = 0$). For example, WN_i interacted with WN_j at time $\{0, t_1, t_2 ... t_{10}\}$, and N_{ij} ranges from 0 to 68. The value of $T_{ij}^{f}(t)$ is shown in Table 1.

4.1.2. Honesty-based social trust factor

The honesty based trust value, $T_{ij}^{h}(t)$, can be used to identify an attacker node by analyzing irregular behaviour. Honesty is a social property which can be calculated from the positive (successful) and negative (failed) interactions of nodes [27]. $T_{ij}^{h}(t)$ defines the level of honesty of the evaluated WN to the evaluated/recommended WNs. Let the positive and negative interactions between WN_i and WN_j be evaluated as αij and β_{ij} respectively and

Table 1: Frequency-based trust value

$Time$	N_{ij}	T_{ij}^{f}
t_0	0	0
t_1	5	0.4467167
t_2	12	0.595939
t_3	19	0.6663576
t_4	26	0.7094014
t_5	33	0.7391797
t_6	40	0.7613517
t_7	47	0.7786867
t_8	54	0.7927211
t_9	61	0.8043848
t_{10}	68	0.814278

the initial value be $T_{ij}^{h}(0) = 0.5$. This means, at time $t = 0$, the wireless nodes WN_i and WN_j have no interaction. $T_{ij}^{h}(t)$ changes with time. Positive interactions raise $T_{ij}^{h}(t)$, while negative interactions lower $T_{ij}^{h}(t)$. In this model, $T_{ij}^{h}(t)$ can be calculated by expectation of beta function as in equation 8.

$$T_{ij}^{h}(t) = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \tag{8}$$

Table 2 shows the effect of positive (α_{ij}) and negative (β_{ij}) interactions on $T_{ij}^{h}(t)$. The evaluation shows that the honesty based trust factor is also a very important parameter for defining the trustworthiness of nodes.

4.1.3. Intimacy-based social trust factor

Intimacy refers to the time an evaluating node WN_i and an evaluated node WN_j have spent communicating between two WNs. The higher the value of spent time, the higher the value of intimacy [39, 38, 40]. In this model, the intimacy based social trust value T_{ij}^{int} measures the level of interaction experiences in terms of time. It can be calculated by the number of interactions between WN_i and WN_j over the maximum number of interactions between WN_i and any neighbouring node WN_k over the time period. Mathematically, T_{ij}^{int} can be calculated by equation (9),

$$T_{ij}^{int}(t) = \begin{cases} 0.5 \text{ for } d = D \\ \frac{d}{D} \text{ else} \end{cases} \tag{9}$$

Table 2: Honesty based social trust factor

α_{ij}	β_{ij}	$T_{ij}^{h}(t)$
1	1	0.5
5	1	0.8333333
5	3	0.625
8	3	0.7272727
15	3	0.8333333
15	10	0.6
20	10	0.6666667
25	20	0.5555556
40	20	0.6666667
80	20	0.8

where $d = \alpha_{ij} + \beta_{ij}$ is the accumulated positive and negative interactions between WN_i and WN_j and $D = \sum_{k=1}^{n} \alpha_{ik} + \beta_{ik}$ represents the accumulation of interactions between node WN_i and any neighbouring node WN_j. $T_{ij}^{int}(0) = 0.5$ when $t = 0$ and $T_{ij}^{int}(t)$ changes with the t when the nodes' interaction increases. Table 3 gives an example of the intimacy factor and how its value changes according to the number of interactions between the evaluating node and other encountered nodes.

Table 3: Intimacy-based social trust factor

N_{ij}	N_{kj}	T_{ij}^{int}
5	7	0.7142857
10	17	0.5882353
20	44	0.4545455
38	60	0.6333333
50	100	0.5
50	280	0.1785714
51	400	0.1275
80	550	0.1454545
90	720	0.125

4.1.4. Energy-based QoS trust factor

The WNs in the MANET environment are energy-constrained nodes and each interaction between the two WNs WN_i and WN_j reduces the nodes' energy. Thus, energy is one of the critical trust factors. In conventional trust models, WNs select neighbour WNs with the highest energy based trust value T_{ij}^{e}, and thus the WN with the highest energy dies quickly in the MANET. Therefore, the trustworthiness of a WN can be evaluated in two ways. Firstly, it can keep good nodes alive for more time, as the evaluation does not depend only on the trust value. Secondly, observing the node energy assists in identifying attacker nodes, as selfish WNs continue to have high levels of energy, while malicious WNs spend more energy in performing attacks. In the proposed model, $T_{ij}^{e}(t)$ indicates the remaining energy level of a WN after each trust update interval t performed by the evaluating WN_i about the evaluated WN_j. The energy factor is calculated as in Eq. (10):

$$T_{ij}^{e}(t) = \frac{E_{ij}(0)}{E_{ij}(t)} \tag{10}$$

where $E_{ij}(0)$ and $E_{ij}(t)$ are the level of current energy and consumed energy at time t respectively for node WN_j. It is assumed that all the nodes have the same initial energy. Receiving and transmitting packets are the only types of communication which are considered for energy consumption. This means that node energy changes with interaction over time t. The value of the energy factor starts at 1, which refers to a situation where nodes have a full battery, and gradually decreases over time as nodes involve themselves in more communications. Nodes continue to be effective in performing interactions so long as the energy factor is not reduced.

4.2. Path Trust Evaluation

In path evaluation methods, a source node chooses the shortest path which also meets energy and social trust value requirements. The trust value of the relaying nodes is evaluated by both direct and indirect methods, and then two composite metrics are employed to evaluate the L trust value between the S-D pair.

4.2.1. Minimum-based trust factor

In the MANET, the source node evaluates the trust values of all the links between the $S-D$ pair. A link which includes nodes with a trust value less than a specified trust threshold is discarded, as the link is not considered to be trustworthy. The trust threshold value is identified as 0.4 because the optimistic scheme is used, in which all nodes are initially trusted and expected to be well-behaved. The initial trust value is 0.5 at time $t = 0$, which is above the trust threshold. Then, the source node selects an optimal routing link which includes intermediate WNs with minimum trust values. Mathematically, the minimum trust value, $T_{ij}^{m}(t)$, at time t of a link L can be calculated by equation (11).

$$T_{ij}^{m}(t) = \min\{T_{ij} | i, j \in L; j \text{ is the next hop relay node}\} \qquad (11)$$

The evaluation $T_{AF}^{m}(t)$ is explained using Figure 2, where the source WN is A and the destination node is F. Table 4 shows the example of the minimum-based trust factor and product based trust factor evaluation methods with the available links from nodes A to F, as indicated in Figure 2. Although there are five possible paths to the destination, the minimum trust value of the path ($A \to B \to D \to F$) which is based on the trust values of the intermediate nodes $(B, D) = (0.90, 0.70)$ is 0.70 (path # 1). This path is the most trustworthy path between the $S-D$ pair. In the product method, paths 2 and 5 have trust values of 0.38 and 0.36 respectively. These values are less than the trust threshold and thereby considered untrustworthy. However, the trust values of the intermediate nodes of these two paths (i.e. path # 2 and path # 5) are higher than the trust threshold and these intermediate nodes should be included. Meanwhile, our method gives a minimum value for path trust of 0.50, which is considered a trustworthy path because this value is greater than the trust threshold.

Table 4: Minimum-based trust factor and product-based trust factor for calculating path trust

Path #	$A \to F$	Trust value	Minimum method	Product method
1	A→B→D→F	(0.90,0.70)	0.70	0.63
2	A → C → E →F	(0.75,0.50)	0.50	0.38
3	A→C→D→F	(0.75,0.30)	0.30	0.23
4	A→B→C→D→F	(0.90,0.80,0.30)	0.30	0.22
5	A→B→C→E→F	(0.90,0.80,0.50)	0.50	0.36

4.2.2. Closeness centrality-based social trust factor

The closeness centrality metric T_{ij}^{c} measures the degree to which an evaluated WN is adjacent to the evaluating/recommending WNs. This metric is inversely proportional to the sum of the minimum distances between the

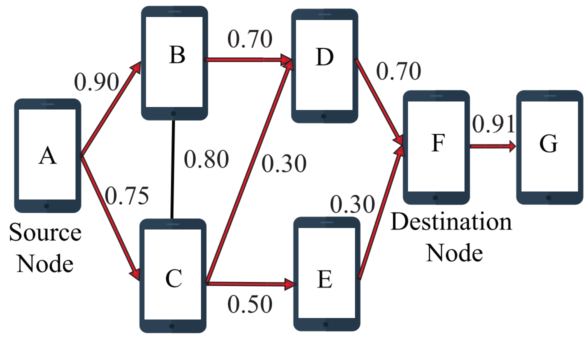


Figure 2: A MANET architecture at time t where node energy is indicated by battery level.

evaluated WN and every other WN in the MANET [28, 32] or hop count or transmission delay (due to distance only). This network parameter is widely used in social networks, describing the efficiency of transmission between an S-D pair. Mathematically, T^c_{ij} can be calculated by equation (12).

$$T^c_{ij} = \frac{1}{\sum_d min(WN_i, WN_j)} \tag{12}$$

In the proposed model, closeness centrality is considered as a measure of the number of hops between an S-D pair. Applying the minimum method, an overall trust value is given to each link, and consequently the link with the maximum trust value is the most trustworthy link. Let us consider the previous example presented in Table 4. Firstly, the minimum distance method is applied, resulting in giving each link between the S-D pair overall trust values of 0.70, 0.50, 0.30, 0.30, and 0.50 for paths 1 to 5 respectively. Secondly, links 3 and 4 are discarded, as the trust value for the link is less than the trust threshold. Thirdly, WN_a appraises links 1, 2 and 5, as their trust value is higher than the trust threshold. Closeness centrality $T^c_{ij} = \frac{1}{2}$ for links 1 and 2 and are considered, as they have minimum hop count. Finally, the trust value of link 1 is higher than the trust value of link 2. Thus, 1 is the most trustworthy link.

5. Simulation and Results

NS2 was used to conduct the simulation for the proposed trust model. This simulator supports MANET architecture through extension of the DSR routing protocol and allows the evaluation of network components like nodes, routing, packets and transport/application layer protocols. The proposed trust model was included in the MANET architecture, wherein the WNs sent the transmission using the DSR routing algorithm.

In the simulator, MANET architecture was created whereby 50 WNs were located randomly in the $700 \times 1000\ m^2$ area. A percentage (e.g. 10 to 50%) of these WNs were considered to be misbehaving nodes which dropped transmitted packets at rates of between 50% and 80%. Also, it was considered that the 15 S-D pairs communicated with each other, and every source generated 2 packets/second (1 packet=512 bytes) for transmission with a Constant Bit Rate (CBR) and a pause time of 60 seconds to their intended destination. The simulation time was considered to be 8.33 minutes. All newly-added WNs were assumed to be trustworthy with $T_{ij} = 0.5$. The threshold trust value was $T_{ij}^{thres} = 0.4$ [41]. The parameters used for configuring the MANET are shown in Table 5.

Table 5: Network Configuration Parameters

Parameter	**Value**
Nodes	50
Area	700 m X 1000 m
Speed	10 m/s
Radio Range	250 m
Movement	Random waypoint model
Routing Protocol	DSR
MAC	802.11
Source-destination pairs	15
Transmitting capacity	2 Kbps
Application	CBR
Packet size	512 B
Simulation time	500 s
Trust threshold	0.4
Fading timer	10s
Deviation threshold	0.5

In the trust model, the selfish nodes drop packets at various percentages, and these nodes generate jamming/collision. It was assumed that 50% selfish nodes were present in the MANET. Bad-mouthing and ballot-stuffing attacks targeted the recommending system by providing dishonest recommendations for the nodes evaluated in the MANET [42]. In these attacks, the recommending system dispensed false recommendations by degrading or promoting trust value of the evaluated node. It was considered that 20% of the recommending nodes were each of these types.

In the simulation, we evaluated three of the QoS parameters, namely network throughput, packet loss and energy consumption for the existing WN, together with misbehaving nodes. The performance of the proposed MANET architecture with the trust model is tested under three cases:

- Case 1: a DSR routing algorithm with no trust relationship between WNs (denoted as DSR);
- Case 2: a DSR routing algorithm with trust relationships between two WNs based on packet forwarding rate (denoted as TDSR); and
- Case 3: a DSR routing algorithm with an energy and social trust-aware trust model (named as proposed).

In all cases, the trustworthiness of a node was evaluated.

5.1. Effect of Misbehaving Nodes on the Performance Metrics

Performance metrics such as the throughput, packet loss and energy consumption of the network were evaluated in the presence of various percentages of misbehaving nodes (10% to 40%).

Figure 3 shows that the overall throughput of the MANET declines linearly with the appearance of misbehaving nodes. In this case, the throughput achieved by the proposed method is highest, while the throughput acquired by the TDSR is moderate compared to DSR.

The effect of various percentages of misbehaving nodes on packet loss is illustrated in Figure 4. The percentage of packet loss rises almost linearly with the percentage appearance of misbehaving nodes for the proposed trust model, TDSR and DSR. In this case, the proposed trust model outperforms TDSR and DSR, whereas the performance of TDSR is moderate compared to DSR.

Figure 5 illustrates the effect of misbehaving nodes on energy consumption for the proposed trust model, TDSR and DSR. The energy consumption rises almost linearly with the percentage appearance of misbehaving nodes. In this case, WNs in the proposed model consume less energy compared to TDSR and DSR.

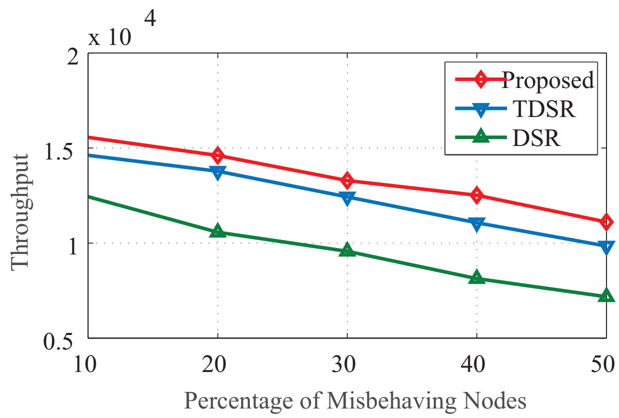


Figure 3: Effect of misbehaving nodes on throughput. An increased percentage of misbehaving nodes reduces the overall throughput of the network for all the three types of routing algorithms.

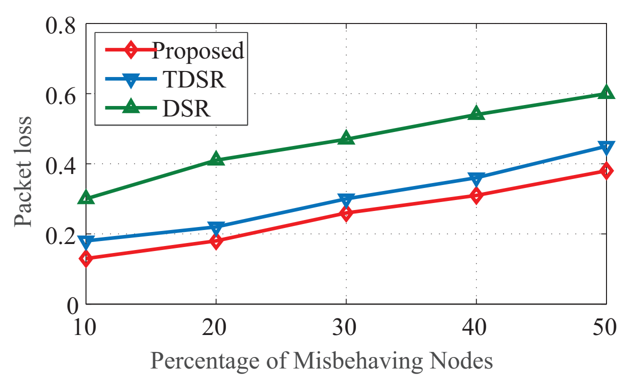


Figure 4: Effect of misbehaving nodes on the packet loss of MANET WNs. For the proposed trust model, TDSR and DSR algorithms, the percentage of packet loss rises almost linearly with the percentage appearance of misbehaving nodes.

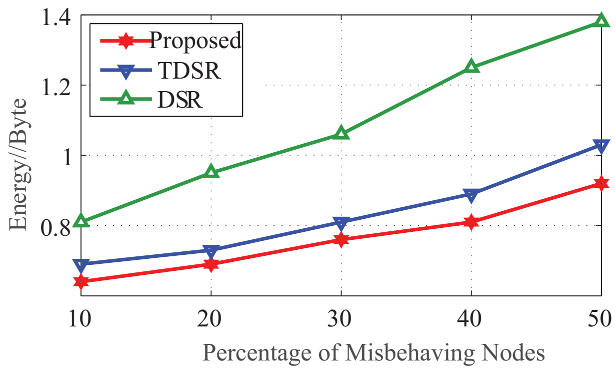


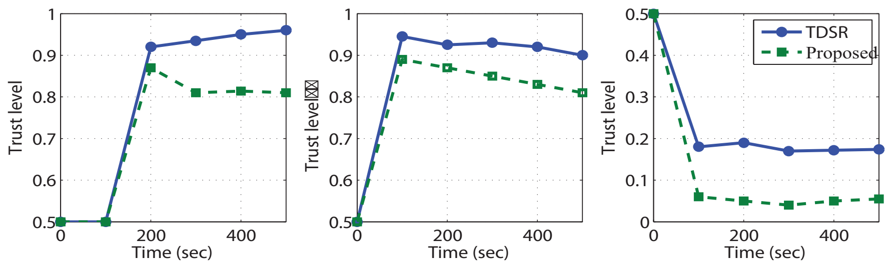
Figure 5: Effect of misbehaving nodes on energy consumption. The energy consumption rises almost linearly with the percentage appearance of misbehaving nodes.

5.2. Effect of Misbehaving Nodes on Trust Level

Figure 6 illustrates the trustworthiness, also called trust level, of good, moderate and bad WNs while attacker nodes coexist with them, for the proposed model and TDSR. Figure 6 (a) shows the trust level for a good node (node 30), which rises with time as the number of favourable interactions with nodes in the network increases. The trust level for the TDSR is higher than that of the proposed trust model. This is because TDSR only uses packet forwarding when evaluating trust value. On the other hand, the proposed trust model includes some social factors to calculate the trust value of an evaluated node. Figure 6 (b) shows the trust level for moderate nodes (node 17), which rises with time as the number of favourable interactions with nodes in the network increases. The trust level achieved for both trust models is less than that for good nodes, as illustrated in Figure 6 (a). Figure 6 (c) shows the trust level of a bad node (node 13). It is obvious that the trustworthiness of bad nodes is the lowest. However, the trust level is higher for TDSR compared to the proposed trust model, as bad nodes require energy resources to conduct such attacks, and also the intimacy of nodes can be low.

5.3. Effect of Social Trust Factors and Energy on Trust Value

The consequence of social trust factors such as frequency of interaction, honesty and intimacy, and energy consumption between the pair of nodes for trust value is illustrated in Figures 7 and 8. Figure 7 shows that trust value changes as the number of interactions increases for frequency of interaction,



(a) Good nodes (b) Moderrate nodes (c) Bad nodes

Figure 6: Effect of misbehaving nodes on the trust level of nodes. (a) good node, (b) moderate node, (c) bad node

.

honesty and intimacy between the pair of nodes. When the frequency of interaction is zero, i.e., no interaction, the trust value is also zero, and this value rises dramatically with increases in interaction and reaches near to 1. Also, the social value increases with the number of honest interactions. Initially, the trust value is not zero, but rather starts from some trust value. However, the trust value fluctuates with the social trust factor called intimacy, which deals with the time spent between two nodes. Thus, this social trust factor has less effect on trust value with increase in the number of interactions between the pair of nodes. Figure 8 demonstrates the effect of energy on trust value. When the number of interactions with the evaluated node rise, energy consumption also increases, and thus the trust value declines linearly.

5.4. Proposed Trust Model versus Service-based Trust Model

The performance of the proposed trust model was compared with the service-based trust model [31] keeping the same network settings. The effect of simulation time and some attacker (bad) nodes on the number of transmitted packets both for the proposed trust model and service-based trust model were studied. Figure 9 (a) illustrates the effect of simulation time on the transmitted packets for various simulation times in the presence of 30% attacker nodes. In contrast to the service based trust model, our proposed model transmitted more packets. The performance degradation for the service-based trust model is due to the selection of attacker nodes in the routing path between source and destination. The proposed model outperformed this model significantly for the entire simulation time and reached 3200 packets towards the later phase of the simulation time, whereas the

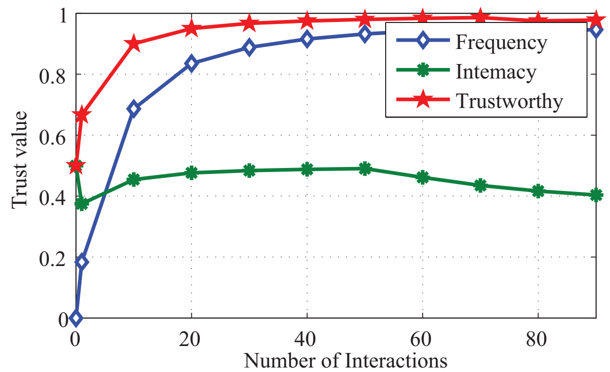


Figure 7: Trust values in relation to the number of successful interactions between evaluating node and evaluated node

.

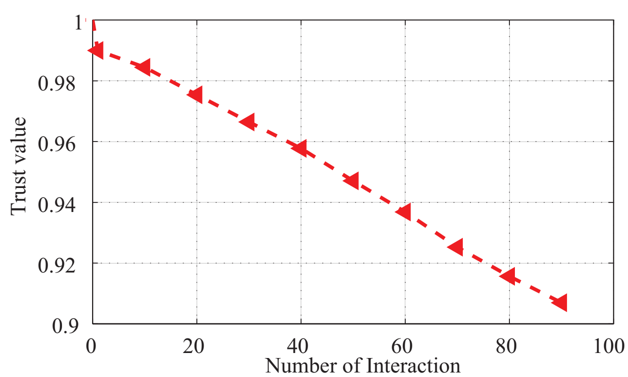


Figure 8: Trust Values as a function of successful interaction between evaluating node and evaluated node for QoS trust value

.

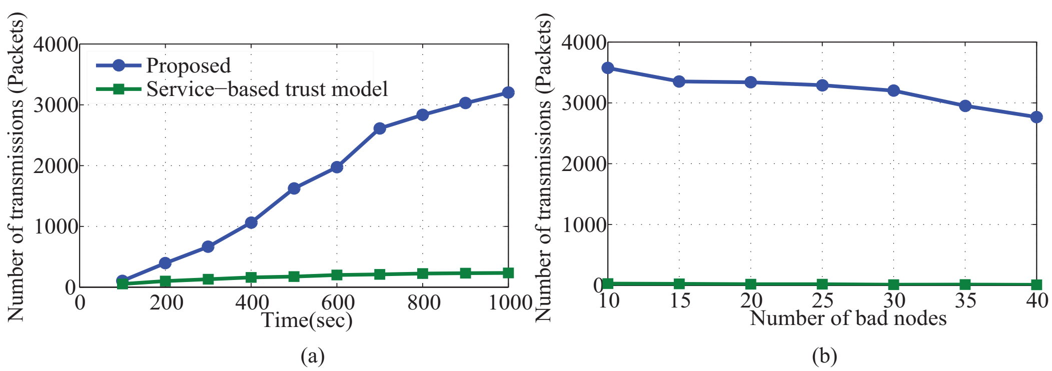


Figure 9: Effect of (a) time (b) number of misbehaving nodes on the packet transmission

.

service-based trust model had reached almost 300 packets towards the end of the simulation. Figure 9 (b) illustrates the effect of some bad nodes in the network on the number of transmitted packets. The proposed model performed better than the service-based trust model in the presence of attacker nodes who drop transmitted packets intentionally. In both models, the number of transmitted packets decreased with the appearance of bad nodes in the MANET. With the arrival of 40% attacker nodes, the number of transmitted packets dropped to just above 2600, from initially more than 3600 for the proposed trust model. In the service-based trust model, the number of transmitted packets was deficient, and stood at less than ten packets at 40% of bad nodes. In summary, the performance of the proposed trust model compared positively to the service-based trust model.

6. Conclusion

In this work, a multidimensional trust model was proposed and analyzed to secure nodes' routing in MANETs based on social properties and QoS factors. A trust model based on one trust metric may not reflect the actual behaviour of nodes and may thus be unable to evaluate the trustworthiness of nodes. Depending on social as well as QoS properties, the proposed trust model evaluates the trustworthiness of wireless nodes in the network. A node's trustworthiness is evaluated by peer-to-peer evaluation and link evaluation. In this trust evaluation model, the performance of the network is evaluated using average throughput in the network, packet loss and energy consumption in the presence of malicious/dishonest nodes. It has been found that the proposed trust model improves the overall performance of the network.

In future, the proposed model can be expanded through additional social properties for identifying node behaviour such as changing identities, malicious behaviour and legitimate new nodes. In addition, adaptive weighting factors can be incorporated to prioritize the effect of these factors over time. Besides this, the proposed model can be compared with other models which utilize both social and QoS factors to validate its robustness over other models available in the literature.

7. References

[1] T. R. Andel, A. Yasinsac, Surveying security analysis techniques in manet routing protocols, IEEE Communications Surveys Tutorials 9 (4) (2007) 70–84. doi:10.1109/COMST.2007.4444751.

[2] F. Aftab, Z. Zhang, A. Ahmad, Self-organization based clustering in manets using zone based group mobility, IEEE Access PP (99) (2017) 1–1. doi:10.1109/ACCESS.2017.2778019.

[3] N. Z. Zenia, M. Aseeri, M. R. Ahmed, Z. I. Chowdhury, M. S. Kaiser, Energy-efficiency and reliability in MAC and routing protocols for underwater wireless sensor network: A survey, J. Network and Computer Applications 71 (2016) 72–85. doi:10.1016/j.jnca.2016.06.005.

[4] G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, Journal of Network and Computer Applications 77 (2017) 48 – 63. doi:https://doi.org/10.1016/j.jnca.2016.10.014.

[5] M. K. Gulati, K. Kumar, A review of qos routing protocols in manets, in: 2013 International Conference on Computer Communication and Informatics, 2013, pp. 1–6. doi:10.1109/ICCCI.2013.6466293.

[6] M. M. Alani, Manet security: A survey, in: 2014 IEEE ICCSCE, 2014, pp. 559–564. doi:10.1109/ICCSCE.2014.7072781.

[7] M. Amadeo, C. Campolo, A. Molinaro, Forwarding strategies in named data wireless ad hoc networks: Design and evaluation, Journal of Network and Computer Applications 50 (2015) 148 – 158. doi:https://doi.org/10.1016/j.jnca.2014.06.007.

[8] G. M. Borkar, A. R. Mahajan, A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks, Wireless Networks 23 (8) (2017) 2455–2472. doi:10.1007/s11276-016-1287-y.

[9] J. Cordasco, S. Wetzel, Cryptographic versus trust-based methods for manet routing security, Electronic Notes in Theoretical Computer Science 197 (2) (2008) 131–140.

[10] H. Yu, S. Liu, A. C. Kot, C. Miao, C. Leung, Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks, in: 2011 IEEE 13th International Conference on Communication Technology, 2011, pp. 1–6. doi:10.1109/ICCT.2011.6157821.

[11] A. M. Shabut, K. Dahal, I. Awan, Friendship based trust model to secure routing protocols in mobile ad hoc networks, in: 2014 International Conference on Future Internet of Things and Cloud, 2014, pp. 280–287. doi:10.1109/FiCloud.2014.51.

[12] A. M. Shabut, K. Dahal, I. Awan, Enhancing dynamic recommender selection using multiple rules for trust and reputation models in manets, in: 2013 IEEE 25th International Conference on Tools with Artificial Intelligence, 2013, pp. 654–660. doi:10.1109/ICTAI.2013.102.

[13] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, A. Hussain, A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications, Cognitive Computationdoi:10.1007/s12559-018-9543-3.

[14] S. Marti, T. J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, MobiCom '00, ACM, New York, NY, USA, 2000, pp. 255–265. doi:10.1145/345910.345955.

[15] P. Michiardi, R. Molva, Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks, in: Advanced Communications and Multimedia Security, IFIP The International Federation for Information Processing, Springer, Boston, MA, 2002, pp. 107–121.

[16] G. Thanigaivel, N. A. Kumar, P. Yogesh, Truncman: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network, in: Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on, 2012, pp. 261–266. doi:10.1109/DICTAP.2012.6215430.

[17] X. Li, F. Zhou, X. Yang, A multi-dimensional trust evaluation model for large-scale p2p computing, J. Parallel Distrib. Comput. 71 (6) (2011) 837–847. doi:10.1016/j.jpdc.2011.01.007.

[18] D. Katsaros, N. Dimokas, L. Tassiulas, Social network analysis concepts in the design of wireless ad hoc network protocols, IEEE Network 24 (6) (2010) 23–29. doi:10.1109/MNET.2010.5634439.

[19] J.-H. Cho, A. Swami, I.-R. Chen, Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks, Journal of Network and Computer Applications 35 (3) (2012) 1001 – 1012, special Issue on Trusted Computing and Communications. doi:https://doi.org/10.1016/j.jnca.2011.03.016.

[20] G. Xu, Z. Yan, A survey on trust evaluation in mobile ad hoc networks, in: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, MobiMedia '16, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2016, pp. 140–148.

[21] A. A. Pirzada, C. Mcdonald, Trust Establishment In Pure Ad-hoc Networks, Wireless Personal Communications 37 (1-2) (2006) 139–168. doi:10.1007/s11277-006-1574-5.

[22] I. R. Chen, J. Guo, F. Bao, Trust management for soa-based iot and its application to service composition, IEEE Transactions on Services Computing 9 (3) (2016) 482–495. doi:10.1109/TSC.2014.2365797.

[23] J. Mundinger, J.-Y. Le Boudec, Analysis of a reputation system for mobile ad-hoc networks with liars, Perform. Eval. 65 (3-4) (2008) 212–226. doi:10.1016/j.peva.2007.05.004.

[24] P. B. Velloso, R. P. Laufer, D. D. O. O. Cunha, O. C. M. B. Duarte, G. Pujolle, Trust management in mobile ad hoc networks using a scalable

maturity-based model, IEEE Transactions on Network and Service Management 7 (3) (2010) 172–185. doi:10.1109/TNSM.2010.1009.I9P0339.

[25] Y. Yu, K. Li, W. Zhou, P. Li, Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications 35 (3) (2012) 867 – 880, special Issue on Trusted Computing and Communications. doi:https://doi.org/10.1016/j.jnca.2011.03.005.

[26] A. Agrawal, A. K. Verma, A review & impact of trust schemes in manet, in: Proceedings of the International Conference on Advances in Information Communication Technology & Computing, AICTC '16, ACM, New York, NY, USA, 2016, pp. 26:1–26:7. doi:10.1145/2979779.2979805.

[27] W. Li, A. Joshi, T. Finin, Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach, in: 2010 Eleventh International Conference on Mobile Data Management, 2010, pp. 85–94. doi:10.1109/MDM.2010.57.

[28] H. Xia, J. Yu, C. liang Tian, Z. kuan Pan, E. Sha, Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks, Journal of Network and Computer Applications 62 (2016) 112 – 127. doi:https://doi.org/10.1016/j.jnca.2015.12.005.

[29] F. Yunfang, Adaptive trust management in manet, in: 2007 International Conference on Computational Intelligence and Security (CIS 2007), 2007, pp. 804–808. doi:10.1109/CIS.2007.80.

[30] F. Li, J. Wu, Uncertainty modeling and reduction in manets, IEEE Transactions on Mobile Computing 9 (7) (2010) 1035–1048. doi:10.1109/TMC.2010.44.

[31] L. Yu, C. Qian, Z. Liu, K. Wang, B. Dai, Ad-hoc multi-dimensional trust evaluation model based on classification of service, in: 2010 5th International ICST Conference on Communications and Networking in China, 2010, pp. 1–5.

[32] Y. Wang, I. R. Chen, J. H. Cho, A. Swami, K. S. Chan, Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks, IEEE Transactions on Services Computing 10 (4) (2017) 660–672. doi:10.1109/TSC.2015.2491285.

[33] J. Guo, I.-R. Chen, J. J. P. Tsai, A survey of trust computation models for service management in internet of things systems, Computer Communications 97 (Supplement C) (2017) 1–14.

[34] A. B. Paul, S. Biswas, S. Nandi, S. Chakraborty, Matem: A unified framework based on trust and mcdm for assuring security, reliability and qos in dtn routing, Journal of Network and Computer Applications 104 (2018) 1 – 20. doi:https://doi.org/10.1016/j.jnca.2017.12.005.

[35] A. M. Shabut, K. P. Dahal, S. K. Bista, I. U. Awan, Recommendation based trust model with an effective defence scheme for manets, IEEE Transactions on Mobile Computing 14 (10) (2015) 2101–2115. doi:10.1109/TMC.2014.2374154.

[36] A. M. Shabut, K. Dahal, Social factors for data sparsity problem of trust models in manets, in: 2017 International Conference on Computing, Networking and Communications (ICNC), 2017, pp. 876–880. doi:10.1109/ICCNC.2017.7876247.

[37] A. Josang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644. doi:10.1016/j.dss.2005.05.019.

[38] E. M. Daly, M. Haahr, Social network analysis for information flow in disconnected delay-tolerant manets, IEEE Transactions on Mobile Computing 8 (5) (2009) 606–621. doi:10.1109/TMC.2008.161.

[39] N. Vastardis, K. Yang, Mobile social networks: Architectures, social properties, and key research challenges, IEEE Communications Surveys Tutorials 15 (3) (2013) 1355–1371. doi:10.1109/SURV.2012.060912.00108.

[40] F. Bao, I. R. Chen, M. Chang, J. H. Cho, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE Transactions on Network and Service Management 9 (2) (2012) 169–183. doi:10.1109/TCOMM.2012.031912.110179.

[41] R. Li, J. Li, P. Liu, J. Kato, A novel hybrid trust management framework for manets, in: 2009 29th IEEE International Conference

on Distributed Computing Systems Workshops, 2009, pp. 251–256. doi:10.1109/ICDCSW.2009.20.

[42] Zakirullah, M. H. Islam, A. A. Khan, Detection of dishonest trust recommendations in mobile ad hoc networks, in: Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2014, pp. 1–7. doi:10.1109/ICCCNT.2014.6962994.