Est. 1841 | YORK ST JOHN UNIVERSITY

Usman, Aminu (2018) A Neighborhood-Based Trust Protocol for Secure Collaborative Routing in Wireless Mobile D2D HetNets. International Journal of Computer Science and Information Security (IJCSIS), 16 (4).

Downloaded from: https://ray.yorksj.ac.uk/id/eprint/4437/

The version presented here may differ from the published version or version of record. If you intend to cite from the work you are advised to consult the publisher's version: https://sites.google.com/site/ijcsis/

Research at York St John (RaY) is an institutional repository. It supports the principles of open access by making the research outputs of the University available in digital form. Copyright of the items stored in RaY reside with the authors and/or other copyright owners. Users may access full text items free of charge, and may download a copy for private study or non-commercial research. For further reuse terms, see licence terms governing individual outputs. Institutional Repositories Policy Statement

RaY

Research at the University of York St John

For more information please contact RaY at ray@yorksj.ac.uk

A Neighbourhood-Based Trust Protocol for Secure Collaborative Routing in Wireless Mobile D2D HetNets

Aminu Bello Usman [#1], Jairo Gutierrez [*2] Abdullahi Baffa Bichi [#3]

[#1,*2] *School of Engineering, Computer and Mathematical sciences*
Auckland University of Technology, New Zealand
[1] ausman@aut.ac.nz
[2] jairo.gutierrez@aut.ac.nz

[*3] *Department of Computer Science*
Bayero University, Kano Nigeria
[3] *abbaffa.cs@buk.edu.ng*

***Abstract*—Heterogeneous Device-to-Device mobile networks are characterised by frequent network disruption and unreliability of peers delivering messages to destinations. Trust-based protocols has been widely used to mitigate the security and performance problems in D2D networks. Despite several efforts made by previous researchers in the design of trust-based routing for efficient collaborative networks, there are fewer related studies that focus on the peers' neighbourhood as a routing metrics' element for a secure and efficient trust-based protocol. In this paper, we propose and validate a trust-based protocol that takes into account the similarity of peers' neighbourhood coefficients to improve routing performance in mobile HetNets environments. The results of this study demonstrate that peers' neighbourhood connectivity in the network is a characteristic that can influence peers' routing performance. Furthermore, our analysis shows that our proposed protocol only forwards the message to the companions with a higher probability of delivering the packets, thus improving the delivery ratio and minimising latency and mitigating the problem of malicious peers (using packet dropping strategy).**

Hetrogeneous Networks, Wireless D2D Communications, Trust-Based Protocol, Secure Collabaorative Routing.

I. Introduction

The Heterogeneous (HetNets) Device-to-device (D2D) networks that enable direct communication between nearby mobiles devices is an exciting innovation that facilitates interoperability between critical public safety networks and increases the amount of traffic, quality requirements, and enables new mobile cloud computing demands. Among others, one important feature of D2D communication is the direct communication with the immediate next-hop peer, which in turn, have several advantages such as increasing network spectral efficiency and energy efficiency, and reducing transmission delay. Along with these advantages, the D2D in the heterogeneous network has various anticipated challenges for collaborative routing. For example, a device may or may not cooperate in data forwarding; a device may fail to appropriately participate in collaborative task due to its limited resources, or position in the network. Also, some routing protocols of D2D communications use the assumption, that in a cooperative HetNets environments, a peer with higher trust value can serve as a good potential relay regardless of the peer's connectivity, and the number of neighbours at a time. This, however, may not be a valid supposition in practice. For example in a Delay tolerant network (DTN), a peer with a good record of data forwarding may receive a packet but can fail to forward it on time if there are no immediate neighbours around or if its neighbours are not connected with other peers that can forward the messages to the destination.

Additionally, the ability of the peers in wireless communication settings to transmit the data packet across the network is limited to the proximity between peers' communication ranges and the energy applied by peers when sending data. In such environments, two peers can communicate with each other only when they are in contact (in the same transmission range with each other). That is to say, a peer that is in a strategic location (connected) can have a higher probability of transmitting the data packets across the network.

Thus, the success of collaborative routing in HetNets depends on the extent at which the peers can fully interact with other peers and peers can make a routing decision based on trust, cooperation, and indeed the level of peers' connectivity in the network. The resultant collaborative routing task between the peers empower the peers to engage in greater tasks beyond those that can be accomplished by individual peers in the network [1], and it helps the peers in making collective routing decisions and judgement about the behaviour and actions of other peers in the network. In fact, collaborative routing between the peers improves the D2D Wireless Network efficiency [2] and enables efficient packet routing and data forwarding. At the same time it prevents jamming and minimises end-to-end delay and latency [3] as well as improving the data-centric behaviour of many WSNs applications [4]. In collaborative routing schemes, a peer may altruistically contribute their resources or serve as a good relay peer for the satisfaction of being an active

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

contributor or to gain recognition (increase in popularity or trust level). Also, peers can collaborate and cooperate in the processes of traffic relaying, outlier analysis, or next neighbour selection to maximize total network throughput by using all the available peers for routing and forwarding. This perception made it clear that the more the peers participate positively in the routing processes, the higher the network performance, and the higher the chances for the network to be secured regarding the denial of service attacks (Sybil attacks, blackhole attacks, etc.). However, the collaborative routing mechanism along with its advantages brings in some security issues such as information errors and losses caused by components' failure of peers in the network, external interference, wireless transmission errors and excessive packet drops [5] which can adversely affect the delivery performance of data communication in the network. All these challenges might be related due to the peers' inability to identify an excellent relaying peer while making a routing decision. Therefore, the success of collaborative routing mechanisms used by wireless D2D devices largely depends on the extent at which the peers can make efficient routing decisions through identifying a connected peer that can serve as a good relaying peer in the network. For example, in many D2D networks such as MANET, WSN, VANETs etc. peers are expected to utilize their limited resources (energy) for routing functions (next peer selection, data forwarding etc.) with the probability of higher packets deliverance.

Previous studies have shown that the cooperation, and collaboration enforcement mechanism between the peers using trust and reputation, can increase the network performance and quality of service [6],[7] in the network. Currently, many D2D trusts and reputation models have been proposed in different kinds of literature. Most of the proposed trust and reputation models only consider the models' implementation based on the satisfactory and unsatisfactory behaviour of the peers in providing the valid packets [8] and the use of community-based reputations to estimate the trustworthiness of the peers (peer trust models) [9] to mention but few. However, the modelling of trust and reputation in D2D networks is a critical mission that cannot be accomplished without considering the information processing and communication across the networks and the connectivity between the peers for effectively distributed trust decision making. In this regards, is of great interest to understand how the peers' contacts and connectivity can influence trust decision processes and by extension can influence routing performance. Here, we note that with the short-range wireless transmission ability of the mobile peers, is possible in the absent of global network connectivity, that the mobility pattern of the peers can be exploited for packet transfer between the peers, even though, there might be no end-to-end connectivity.

Further, rescent studies including the work of [10] shows that the network of Mobile HetNets exhibits a ubiquitous of Transient Connected Components (TCCs).That peers make contacts and interact with other peers to form connected components which can enable peers to contact each other through multi-hop wireless connection. Further, some studies inclusing the work of [11] have shown that the use of social metrics and Complex Network Analysis (CNA) such as peers' Centrality Estimation for computing the comparative centrality of two encountering peers and similarity of the peers' behavioural profiles based on the mobility preferences [12], peers' betweenness and community structure [13] can be exploited to provide effective solution to improve the performance of routing forwarding between mobile peers. Further, previous studies suggested that the peers' mobility can equally contribute to predicting peers' contacts, peers connectivity and peers ability in delivering the packets from the sources to the destinations [14]. We understand that the community structure is an essential properties of CNA that reveals the inherent structure of the complex network and can be used for predicting the future contacts in mobile networks such as DTNs MANETs etc [13].

One of the basic measures to describe the peers' network connectivity is the distribution of the number of links (established wireless connections with other neighbours) per network-node and the number of shared neighbours among the peers. However, to investigate peers' connectivity of mobile network settings in relation to routing between the peers, it is essential to understand the basic principles behind peers, contacts, peers' mobility pattern and a key step in establishing contact between peers among the neighbours (discovery process).

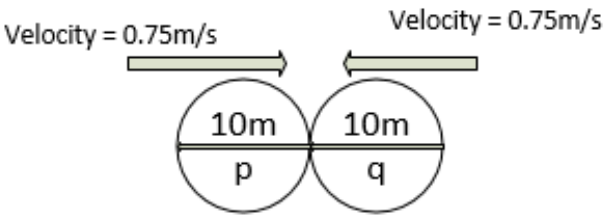

Fig. 1. Contacts Illustration

For example, consider the diagram in Figure 1, which illustrates the encounters between the two mobile peers, p and q who move in opposite directions (toward each other), with each peer having a diameter range of 10m moving at a velocity of 0.75m/s. It can be noticed that the contacts and connectivity between the peers depend on three factors. The first factor is the diameter of the peers (wireless range covered); with a diameter = 10m, it will take the peers a minimum window contact opportunity of only 26.7s to overlap each other (to go out of range of each other), and when the diameter of the devices is 15m each, and with the same velocity of 0.75m/s, the contact opportunity can be up to 40s. Here, we note that the contact time is the time it takes the peers to discover each other and establish a communication channel. Although this

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

is trivial, it can be noticed that the devices' wireless ranges influence the devices' contact duration and connectivity.

The second factor is the speed of the devices. With the increase of the peers' speed, the minimum contact time decreases. The third factor which is related to our interest is the frequency of contacts between the peers (this will be covered in detail in subsequent sections).

However, some of the related questions for understanding the connectivity between peers in relation to forwarding metrics include: how can the peer's contacts be appropriately captured and represented adequately in the neighbours' discovery process for trust evaluations? Can the peers' contacts, motions serve as a basis for peers' connectivity and peers' ranking in trust evaluation metrics? How can the decision trust be integrated with the peers' connectivity ranks for collaborative routing decisions? To attempt these questions, we contribute in the following ways:

(i) We propose a neighbourhood trust-based data forwarding strategy to improve the performance of wireless mobile devices in a HetNets. We achieved this through developing a similarity algorithm for quantifying the peer's similarity regarding the number of neighbours as a forwarding metric.

(ii) We propose a new trust-based protocol for evaluating peers routing behaviour.

(iii) We analyse the relationship between peers' connectivity, peers' radio ranges, and peers' speed for a trust-based routing decisions as a new way of understanding peers' attributes as elements of trust evaluation between wireless peers.

For the experimentation, we observed performance of our proposed solution using the Opportunistic Networking Environment (ONE) Simulator [15].

II. Related work

Several trust-aware models based on routing and resource attributes for peer selection using measures of trustworthiness and peers routing abilities were proposed in the litreture[16]. There are few efforts from the literature that explore the influence of peers' connectivity as a trust evaluation factor in D2D collaborative routing schemes[17]. The use of social properties such as friendship [18], community structure [19], similarities regarding peers' interests [20] and location of peers [21] has recently become the focus of many collaborative routing schemes. Yet, there has been less work dedicated to clearly establish the relationship between different peers' routing elements such as peers' speed, interface range and peers' overlay connectivity in relation to peers routing reliability for trust-based routing protocols.

Further, many of the ad-hoc network trust models are naively based on a trust-your-neighbour relation. In this type of trust model, the entire trust management system (origination, managing and expiration) usually has a short lifespan, and the peers may lack a comprehensive knowledge of the overall neighbour trust level. As a result, most of the direct trust models only work in an environment where all the nodes are self-organized and mobile (e.g., military and law enforcement applications) which limits their functionalities to some specific areas.

Recently, several attempts were made by many authors to propose a different improvement in the various aspects of direct trust and reputation algorithms. For example, the study in [22] introduced a zone-based trust management agreement scheme in wireless sensor networks. The scheme was designed to detect and revoke groups of compromised nodes within the trust formation and forwarding phase. Each node directly interacts with the neighbouring nodes for the trust report event and stores the report in a knowledge cache. The proposed protocol comprises of zone discovery, trust formation and forwarding phases. Before making a final judgement, a trustor will always compute the difference between the probability distribution function of the neighbourhood trust and the probability distribution function of the information received from its neighbours at every slot of time (say, T). The total trust factor can be determined based on the deviation between the reports of the observation using the information theoretic metric KullbackLeibler-divergence.

Also, the work in [23] proposed a novel, Connected Dominating Set (CDS)-based reputation monitoring system. Which employs a CDS-based monitoring backbone to securely aggregate the reputation of sensors without subjecting them to energy depletion or reputation pollution attacks.

In addition, apart from constraints that are application-specific, the concept of direct trust suffers from the following setbacks that may limit its application in a distributed and autonomous wireless network: a) Notion of prediction: peer p can either trust peer q or distrust peer q [24], since it has no other means of trusting peer q; b) peer p can only compute peer qs' trust value under the condition that peer p trusts peer q; c) Energy depletion problem; the amount of energy needed for a wireless node to accomplish trust management processes (trust aggregation and trust evaluation) with all other neighboring peers in a distributed network will be high, since the trust between peers can only be derived based on their direct contacts and the energy needed for the node to communicate with other peers is proportional to its distance with other peers in the network [25].

III. Neighbourhood Connectivity Model

Connectivity and community structure recently became the central focus of behaviour-oriented and opportunistic routing paradigms and delay tolerant networks [26]. Recently, some researchers incorporated Complex Network Analysis (CNA) to formulate and predict the future contact between peers and the peers' reliability and relay selection strategy [27]. The community structure is one of the most important properties of Complex Network Analysis. In a simple terms, a network is said to have community structure if the peers of the network can be easily grouped together into (potentially overlapping) sets of peers and each peer in the network can efficiently interact with other peers either through direct contact or indirect contacts. Based on the previous findings in the literature [17], evidence suggests that to improve routing performance

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

between wireless peers, taking advantage of positive social characteristics such as community structure and friendship to assist packet forwarding is essential. Additionally, the concept of community structure in relation to transitivity also goes in line with the dynamic balance theory and Simmelian triangle theory which states: "The localised cohesion between transitive peers is optimal for sharing information, encouraging cooperation and minimising conflict between the actors" [28]. The tendency for a peer to belong to a certain structured community with a similar neighbourhood can represent its potential reliability to handle a particular task to improve the quality of communication in the network and serve as a relay peer in dealing with the task of packet forwarding. Motivated by the different social network and delay tolerant routing protocols that use the history of the encounter between the peers and the transitivity in estimating each peers' delivery probability. Therefore, due to the uncertainty in nodal mobility, we foresee that identifying a particular node that belongs to a community within an arbitrary mobile wireless network can provide a new angle of view in the design of trust-based routing protocols. Thus, to understand the effects of connectivity as routing attributes, we identify a neighbourhood coefficient as a measure of the degree to which peers in the network tend to cluster together.

Given a network $G = (N, L)$ with peers' sets N and the links between the peers L. Each peer in the network can be a source or destination of the traffic, and with equal transmission range $\iota(n)$. We can define the network as $G = (N, L) : N = \{p, q, ..., r\}$ and $L \subseteq \{(p, q)\} : p, q \in N$, and $p \neq q$. Let the transmission range of peer p be $\iota(p)$ and the distance between peer p and peer q be $dis_{p,q}$. Let n_p denotes the set of peers that are neighbours of peer p and within the communication area of p. For the communication between peer p and peer q to be successful the following condition must be satisfied: (i) $dis_{p,q} \leq \iota(n)$ (receiver is within the communication range of the sender) and any peer r such that $dis_{r,q}\iota'(r)$, is not transmitting (i.e, the receiver is free of interference from any other possible sender). In other words, peer p can successfully transmit the packet to q if p is a neighbour of q and no other q's neighbour is transmitting to peer q simultaneously.

A. Neighbourhood Coefficient Approximation

Given a network $G = (N, L)$ consisting of peers $N = \{p, q, r\}$ and the set of communication links between the peers $L \subseteq \{(p, q)\} : p, q \in N$, and $p \neq q$, the set of neighbourhood of peer p is defined as its immediately connected neighbours as follows $N_p : N_p = \{q : \{(p, q)\} \in L \wedge \{(q, p)\} \in L\}$. If $\{(p, q)\}$ is distinct from $\{(q, p)\}$, for each peer $p \in N$ there are possible number of distinct wireless interface connection $n_p(n_p - 1)$ that could exist among the peers within the neighbourhood of peer p, where n_p is the total number of peer p neighbours.

Therefore, if we denote the neighbourhood coefficient of peer p as $N_{coef(p)}$, we can compute the routing metric of peer p using the following clustering coefficient equation (1).

$$N_{coef(p)} = \frac{2\{|\{p, q\} : p, q \in N_p, \{(q, p)\} \in L|\}}{(n_p(n_p - 1))} \quad (1)$$

Figure 2 shows an example of a community neighbourhood network of nine peers with their corresponding neighbourhood coefficient in Table I using equation (1). Suppose that peer p have a data to forward to the destination in the form of "store-carry-and-forward". Based on the existing trust mechanism in the literature, peer p can forward the packets to a peer with the higher trust value among y, f and r whose have a direct contact (indicated line between the peers) with peer p. We used the clustering coefficient equation (1) to compute the peer's neighbourhood coefficient of Figure 2 to arrived at Table I. Looking at Table I, since peer r has higher forwarding metrics regarding connectivity, it may have a higher chance of routing to the destination.Thus, it might be additional routing intelligence if peer p can evaluate its subjects' neighbourhood coefficient as an additional element of trust evaluations.

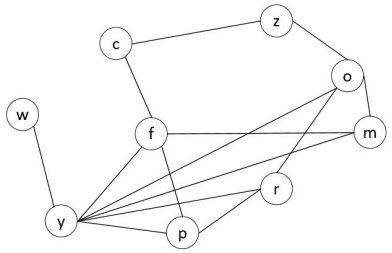

Fig. 2. Neighbourhood Illustration

TABLE I
FORWARDING METRICS TABLE

Peers	$N_{coef(p)}$	$N.Pairs = \frac{n_p(n_p-1)}{2}$
w		0.000
z	0.000	1.000
c	0.000	1.000
o	0.333	6.000
y	0.333	15.000
m	0.667	3.000
f	0.333	6.000
r	0.667	3.000
p	0.667	3.000

B. Neighbourhood Similarity Modelling

The similarity in terms of frequent contacts, visited locations or interests are often seen as major factors for connectivity in DTN and social networks. For instance, people tend to connect with those sharing similar tastes, social background, interests and beliefs, and also similar popularity. This is often expressed as "love of the same" or "Birds of a feather flock together" [29]; that is the tendency of individuals to associate and bond with similar others which can be treated synonymously with similarity in the context of connectivity. On the same vein, peers' similarity as a network formation model can also reproduce the commonly perceived power-law or scale

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

free distribution of sparsely connected networks. It should be clear that in a traditional random network the degrees of all peers are distributed around the average [30], therefore using similarity of peers degree can equally be applied in collective or collaborative routing for behaviour analysis and outlier analysis for networks anomaly identification. Subsequently, a similarity model can produce the characteristics of different densities in real networks, thus, it can be used as a model for describing the topological transition between the peers in the network [31]. Therefore, the tendency of a peer to belong to a certain structured community with a similar neighbourhood can represent its potential routing ability for data forwarding within the community thus, will improve the quality of communication in the network [32]. Additionally, motivated by different social networks and delay tolerant routing protocols [33] that use the history of encounters and similarity between the peers in terms of frequent visited locations and mobility patterns for predicting peers' delivery probability, we proposed a connectivity similarity model . In this regard, we postulate that the relative comparisons of the proliferation of peers' transitivity coefficients may give a meaningful basis for understanding the peers' connectivity for collaborative routing handling [34]. We envision that such comprehensive approach has two advantages:

1. It stimulates behaviour-aware message routing protocol thereby each peer can understand the changes of its potential routing partners' connectivity; thus determining whether a peer will be a good relaying peer or otherwise.

2. It also speeds up the discovery of the peer with similar behaviour and mobility pattern for collaborative routing decisions.

Thus each time peer p wants to participate in a routing process, it will advertise its neighbourhood coefficient. This can be achieved through simple scanning of its neighbours.

$$d(N_{coef(p)}, N_{coef(q)}) = |N_{coef(p)} - N_{coef(q)}| \tag{2}$$

We can, therefore, normalise the difference between the two possible attributes values with the maximum possible attributes level as follows.

$$d(N_{coef(p)}, N_{coef(qi)}) = \sum_{i=1}^{n} \frac{|N_{coef(pi)} - N_{coef(qi)}|}{Max(N_{coef(pi)}, N_{coef(qi)})}, \tag{3}$$

Therefore, the similarity between peer p and q's neighbourhood coefficients can be evaluated as: $S_{p,q} = 1 - d(N_{coef(p)}, N_{coef(q)})$ which can be represented as follows:

$$S_{p,q} = 1 - \sum_{i=1}^{n} \frac{|N_{coef(pi)} - N_{coef(qi)}|}{Max(N_{coef(pi)}, N_{coef(qi)})} \tag{4}$$

From equation (1), the $Max(N_{coef(pi)}, N_{coef(qi)}) = 1$, therefore, the similarity between peer p and peer q is simply $1 - \sum_{i=1}^{n} |N_{coef(pi)} - N_{coef(qi)}|$. We can simplify the similarity of peers' neighborhood coefficient using the following equation (5).

$$S_{p,q} = 1 - |N_{coef(p)} - N_{coef(q)}| \tag{5}$$

IV. Trust Model

In this section, we describe the trust evaluations between mobile peers. Upon an encounter between two peers (p, q), peer p can update its direct trust on peer q based on the update of the total. For example, let $t_{p,q}$ be the trust value that peer p places in peer q based on its a priori experience with peer q, where $t_{p,q} \in \langle 0, 1\rangle : p \neq q$. Looking at the distributes *EigenTrust* algorithm [8], each time peer p encounters peer q, peer p can assess the trust level of peer q based on their encounter delivery vectors exchanges. If the encounters history is not satisfactory it will be considered as a negative experience, therefore the local trust value $(t_{p,q})$ between p and q will decrease; while if the encounter history between the peers is satisfactory, then it will be considered a positive experience and the $(t_{p,q})$ will increase. If the peers' transaction is undecided, it will have no effect in the peers' trust evaluation. Therefore, $sat(p, q)$ represents the number of satisfactory encounters between peer p and peer q while $unsat(p, q)$ represents the total number of unsatisfactory encounters between peer p and peer q[35]. Evidence of trustfulness is manifested by the encounters history exchanges between the peers. Thus, the resultant local trust value between the peers can be computed as $C_{p,q} = sat(p, q) - unsat(p, q)$. The normalised reputation can be computed as:

$$t_{p,q} = \frac{max(C_{p,q}, 0)}{\sum_q max(C_{p,q}, 0)}, ||\vec{t_p}|| : \sum_{q=1}^{N} t_{p,q} = 1 \tag{6}$$

The global trust equation peer p can estimate about peer r based on the feed back of peer q about the behaviour of peer r can be presented in the following equation (7).

$$T_{p,q} = \sum_{q} t_{p,q} t_{q,r} \tag{7}$$

Therefore, each peer will maintain the local trust observation vectors of its subjects' trust values as follows:

$$\vec{t_p} = (t_{p,q}, ..., t_{p,N})^T, 0 \leq t_{p,q} \leq 1 \tag{8}$$

Note: the local trust value $(t_{p,q})$ in equation (8) represents the normalised local trust value peer p have about q and other peers in the network; $T_{p,r}$ in equation (7) is global (transitive trust) of q computed by p based on trust that p has about q. Therefore, every peer can use his global observation vector's elements $(\vec{t_p})$ to compute the global trust value $T_{p,q}$. To secure the implementation of our protocol, we estimate the trust value of the peers to two basic principles; (1) the trust value of a peer is computed in a distributed fashion. Thus a peer does not have access to its trust information where it can be subject to alterations and (2) the trust value of a peer is computed by more than one peer so that malicious peers cannot succeed in white washing attacks.

The above presented algorithm is used to determine the trust worthiness of a peer in delivering received messages.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

For instance, peer p can assess peer q's unhealthiness based on evidence manifested due to malicious attacks detected which including packet dropping, self-promoting, bad-mouthing and ballot stuffing attacks through the encounter history exchanged from peer q. In the event where the encounter history is satisfied (e.g., using encounter tickets as in [36]), this is considered as a positive experience which can cause an increase in the trust level of q in the eyes' of p, otherwise it is considered as a negative experience which can lead to the decrease in the trust level of q .

Based on peer p's experience about q, peer p can store the trust value of peer q and the neighbourhood coefficient similarity value with peer q: $(T_{p,q}, S_{p,q})$ after every contact between the two peers. If peer p has not stored $(T_{p,q}, S_{p,q})$, the trust value between the two peers is assumed to be zero therefore, the trust value can be recalculated at each opportunistic encounter according to the following rules:

1) All peers enter the mode where they can search for their neighbours using their shortest range receivers.
2) On finding one or more peers within the transmission range a peer can search its contact list to find the trust value of a peer and compute the corresponding neighbourhod similarity with the encountered peer before data transfer.
3) Every peer keeps its neighbourhood list and their corresponding trust values and adds itself as a member.
4) Peers keeps on exchanging their neighbourhod list.

Therefore, we define a specific function $TS(T_{p,q}, S_{p,q})$ as the resultant trust value between the peers as follows in equation (9).

$$TS = T_{p,q} * S_{p,q} \tag{9}$$

Our proposed connectivity trust model enables a peer to route a data packet to the corresponding neighbour with the higher probability of delivering the data packet to the destination. As mentioned earlier, the neighbours (connected peers) of the forwarding peer are those that are in the same transmission range with the forwarding peer with each node having a unique identifier. Once a peer is in the position to forward the data packet, it will look into its routing list for the computation of the trust value of its neighbours. The inputs to the routing decision depend on both the trustworthiness of a peer and the similarity of the peers' connectivity. This is to enable us to explore the relative effect of the peers connectivity in terms of routing handling. Once a peer aggregates all the trust values it will then filter peers' trust values and rank them before forwarding to the routing engine for a routing decision. A peer will select an optimal next-hop node from its neighbours using the resultant computed trust values.

Based on the presented trust model, one can observe that in an ideal collaborative wireless mobile environment, all peers can choose a next-peer for routing based on their similarity in terms of connectivity and the trustworthiness of a peer in terms of reliability for routing handling; in that way a routing path can be optimised based on the peers' trustworthiness and peers' connectivity; thus a simple connectivity trust-based protocol is achieved.

V. Protocol Implementation

We understand that DTNs, posses most of the characteristics of wireless D2D HetNets. Therefore, throughout this paper, we consider the characteristics of DTN networks for presenting our concept. However, our proposed model can be applied to different scenarios and related applications.

To avoid routing loops, we consider a three-hop counts routing mechanism. i.e, the maximum number of hop-counts a packet can visit is limited to only 3 hops between the source and the destination. We achieve this through configuring the TTL (Time-to-Live) value of the packets so that as the packet move between hops, the packet's TTL field is decrease by one. In the event where the TTL value reaches 0, the packet is dropped by the relaying peer that decrease the value from 1 to 0.

We conducted simulations using Opportunistic Network Environment Simulator [15] which is a DTN simulator popularly known for modelling the behaviour of store-carry-forward networks [37], [38]. We assume peers' discovery takes only 40 seconds and the packet transfer depends on the resources' availability of buffer, energy, bandwidth, and Time To Leave (TTL) etc. A peer is choose as a message carrier if its trust value is higher in comparison with other peers and its connectivity with other peers is similar to that of the sending peer. A peer must also posses the trust threshold i.e., a minimum trust level required for a peer to participate in collaborative routing. At the initial stage, we implemented our trust model with the pre-trusted peers percentage, pre-trusted peers weight and zero trust node selection probabilities as presented in Table II.

A. Protocol Evaluation

We first seek to understand how the peers connectivity influences the peers' trust evaluation in mobile wireless environments. We thus simulate the peers' mobility pattern at varying speeds of $0.5m/s$ and $0.75m/s$ as shown in Figures 3, 4, Figure 5. In our simulation, as the peers move around, they keep having contacts with other peers and interact (establish contacts, exchange messages, etc). The level of peers interaction determine its connectivity which by extension influences the performance of the routing protocol[39]. Subsequently, we model the average percentage of distinct neighbours encountered both directly and through indirect contacts. For the indirect connectivity case, we mean the peers that are reachable via multi hop relay through neighbours' neighbours as in [40].

The graph of Figure 3 shows that the average distinct number of peers connected. The plot shows as the radio ranges of peers (interface range) and movements speed increases, the peers' direct and indirect connectivity of peers increases as well. The results revealed that the faster-moving peer have

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE II
IMPLIMENTATION PARAMETERS

Number of host	50
Number of interface per peer	2
Movement model	Shortest path map based movement
Peers buffer size	50M
Peers' interface	Blue tooth
Message sizes	(500kB - 1MB)
Peers percentage	0.3
Pre-trusted peers weight $(init)$	0.25

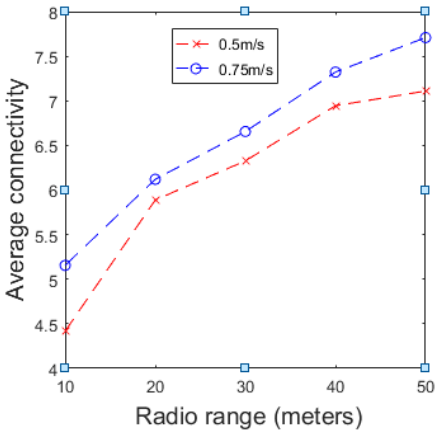

Fig. 3. Average distinct connected neighbours

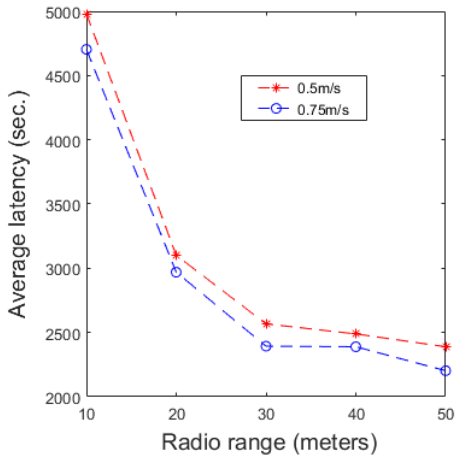

Fig. 5. Average latency in relation to peers' radio ranges

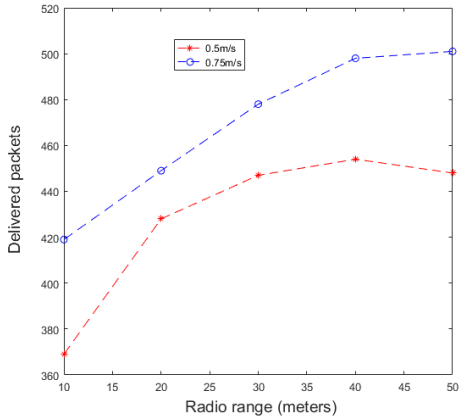

Fig. 4. Delivered packets in relation to peers' radio ranges

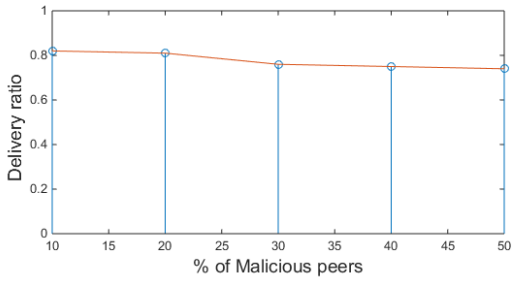

Fig. 6. Delivery ratio under best trust formation

higher chances of meeting many other peers and establish connectivity with them. The results further show that, peer-to-peer protocols can exploit the indirect connectivity (transitivity) to reduce the radio ranges in sparse networks thus, reducing the energy required for message transmission. The graph in Figure 4 further shows the number of delivered packets in relation to the increase of peers' interface ranges. The graphs shows that with the increase in peers interface ranges, the number of packets successfully delivered is increasing. In other words the total number of packets received by all the peers in the network. The higher the number of packets delivered the higher the performance of the protocol. From the presented results shown in Figure 4, one can observe that there is a significant improvement in the number of packets delivered with the increase in the peers' speed. It is important to emphasise here that the number of packets delivered in collaborative networks is closely associated with quality of service considerations, and it is related to reliable network performance.

These results support our arguments that the peers' connectivity is an important factor for efficient trust evaluation between peers in the network. The results further support that, if highly connected peers can determine their corresponding

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

neighbouring peers with similar a connectivity index, the peers collaborative routing performance can be enhanced. In the next subsection, we proceed to evaluate our proposed protocol based on the peers' connectivity similarity for trust evaluation.

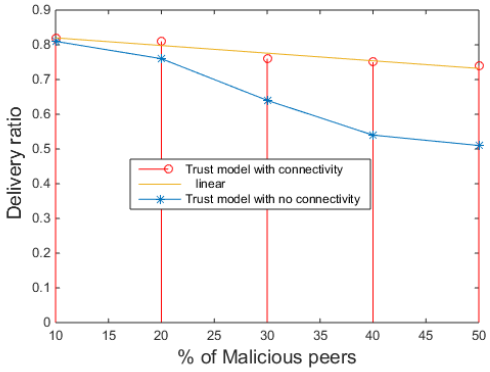

Fig. 7. Benefit of Trust Based Peer Selection Strategy

Next, we focus our attention to the trust evaluation used to optimise the routing performance and to diminish the effect of selfish behaving peers. We consider one of the most important performance metrics (delivery ratio) for the secure implementation of D2D routing protocols. We assigned certain percentage of peers to be periodically dropping the received messages. The malicious peers have limited transmission ranges and buffer sizes. This induces the malicious peers to frequently drop the received packets. We also limit the TTL of the packets created by malicious peers to be 2 minutes only, while for the good behaving peers is up to 300 minutes. This is to enable us to model the behaviour of peers serving as malicious peers. Once the prescribed time count(2 minutes) for packets from malicious peers has elapsed, the peers can discard the packets. Therefore, the number of malicious packets is limited. This is a typical denial-of-service attack which degrade the quality of communication between the peers and reduces network performance. This type of attack can occur due to several reasons; peers being compromised by attackers, peers malfunctioning or any selfish behaviour that can warrant a peer to refuse to participate in packet forwarding. Our goal is to find the best way for peers to identify reliable trustworthy peers for message deliverance.

The experiment proceeds by repeatedly increasing the percentage of malicious peers who drop the received packets frequently. From the result of the experiment, fig 6 shows the maximum delivery ratio obtained when the trust algorithm operates under the best trust formation settings identified in table II. We account the delivery ratio as the total number of packets sent by all the peers in the network divided by the total number of packets received by the all the peers in the network.

We see that the delivery ratio remains higher even when the percentage of malicious peers keeps increasing. This to some extent shows the resilience of our proposed connectivity trust model with the increase in malicious peers.

We then proceed to conduct a comparative analysis, contrasting between the trust model with connectivity scaling factor and a trust model with no connectivity scaling factor. From the graph in Figure 7, it can be observed that the packets delivery probability of the trust model with connectivity scaling factor shows a significant improvement with the increase in malicious peers. However, the delivery probability of a trust model with no connectivity scaling factor show the worst performance.

From the graph in Figure 7, we can deduce that, the implementation of our proposed trust model (with connectivity) exhibits higher performance in comparison with a trust model with no connectivity in terms the packets delivery ratio. For instance, the graph shows a linear slight decrease of delivery ratio with respect to the increase in malicious peers. The result also revealed that the inclusion of connectivity as an element of trust evaluation between the peers improve the peers trust evaluation thus, peers can identify the best possible neighbours to interact with.

Moreover, since the delivery probability favours the increase in the similarity of the connectivity, and the fact that the connectivity between the peers determine the delivery performance, this shows that even in the sparse network, our proposed trust model based on connectivity can yield a good performance in determining the best possible peers to collaborate.

VI. Conclusions and Future Work

The paper has presented a trust-based scheme that exploits peers' neighbourhood characteristics to achieve secure and efficient forwarding strategy among peers in D2D HetNEts. Our proposed solution combines the peers' trustworthiness and similarity of peers' neighbourhood coefficient for trust evaluation. Our trust-based protocol design allows the peers to identify the best possible peer to interact in the midst of the peers while moving to maximise the packets delivery and minimise latency. The result of this study, backed by the simulation validation, demonstrated that there is a correlation between peers' connectivity, peers' interface ranges, and peers' speed and those factors can be used for modelling peers' routing behaviour. We understand that as the peers' radio interface increase and peers' speed increases, the peers tend to establish connectivity and transfer messages with less latency and the routing performance keep increasing. Further, the result validation shows that our proposed solution is resilient against malicious peers and achieves higher performance of packet delivery ratio. Although our proposed trust-based routing protocol development is still very much underway, we discern that the preliminary stage presented in this paper may be useful to any ad-hoc networking protocol design. It shows a new way of interpreting peers connectivity and offers insight into how peers' neighbourhood coefficient can be interpreted as an additional scaling factor for trust and reputation protocol design. Based on the presented study in

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

this paper many questions need further investigation about the peers' characteristics that can improve peers' routing decision. In the next step of this research, we intend to improve our knowledge about how the three parameters: connectivity, peers' interface range and speed can be modelled to understand peers dynamic motion and behaviour for peers' reciprocity and altruism in trust-based routing.

REFERENCES

[1] Praveen Jayachandran and Matthew Andrews. Minimizing end-to-end delay in wireless networks using a coordinated edf schedule. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.

[2] Dayong Ye, Minjie Zhang, and Yun Yang. A multi-agent framework for packet routing in wireless sensor networks. *Sensors*, 15(5):10026–10047, 2015.

[3] Maggie X Cheng, Xuan Gong, Yibo Xu, and Lin Cai. Link activity scheduling for minimum end-to-end latency in multihop wireless sensor networks. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5. IEEE, 2011.

[4] Ángel Cuevas, Manuel Urueña, Gustavo De Veciana, Rubén Cuevas, and Noël Crespi. Dynamic data-centric storage for long-term storage in wireless sensor and actor networks. *Wireless networks*, 20(1):141–153, 2014.

[5] Yan Sun, Hong Luo, and Sajal K Das. A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks. *IEEE Transactions on Dependable and Secure Computing*, 9(6):785–797, 2012.

[6] Aminu Bello Usman and Jairo Gutierrez. A reliability-based trust model for efficient collaborative routing in wireless networks. In *Proceedings of the 11th International Conference on Queueing Theory and Network Applications*, QTNA '16, pages 15:1–15:7, New York, NY, USA, 2016. ACM.

[7] Jaydip Sen. *Reputation-and trust-based systems for wireless self-organizing networks*. Aurbach Publications, CRC Press, USA, 2010.

[8] Sepandar D Kamvar, Mario T Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651. ACM, 2003.

[9] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *Knowledge and Data Engineering, IEEE Transactions on*, 16(7):843–857, 2004.

[10] Xiaomei Zhang. *Efficient and Quality-Aware Data Access in Mobile Opportunistic Networks*. PhD thesis, The Pennsylvania State University, 2016.

[11] Peiyan Yuan, Huadong Ma, Xiang-Yang Li, Shaojie Tang, and Xufei Mao. Opportunistic forwarding with partial centrality. *arXiv preprint arXiv:1208.0186*, 2012.

[12] Wei jen Hsu, Debojyoti Dutta, and Ahmed Helmy. 1 csi: A paradigm for behavior-oriented profile-cast services in mobile networks.

[13] Bing Bai, Zhenqian Feng, Baokang Zhao, and Jinshu Su. Benefiting from the community structure in opportunistic forwarding. *Comput. Sci. Inf. Syst.*, 10(2):865–876, 2013.

[14] Azzedine Boukerche and Amir Darehshoorzadeh. Opportunistic routing in wireless networks: Models, algorithms, and classifications. *ACM Comput. Surv.*, 47(2):22:1–22:36, November 2014.

[15] Ari Keränen, Jörg Ott, and Teemu Kärkkäinen. The one simulator for dtn protocol evaluation. In *Proceedings of the 2nd international conference on simulation tools and techniques*, page 55. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[16] Aminu Bello, William Liu, Quan Bai, and Ajit Narayanan. Revealing the role of topological transitivity in efficient trust and reputation system in smart metering network. In *Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on*, pages 337–342. IEEE, 2015.

[17] Ying Zhu, Bin Xu, Xinghua Shi, and Yu Wang. A survey of social-based routing in delay tolerant networks: positive and negative social effects. *IEEE Communications Surveys & Tutorials*, 15(1):387–401, 2013.

[18] Eyuphan Bulut and Boleslaw K Szymanski. Friendship based routing in delay tolerant mobile social networks. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5. IEEE, 2010.

[19] Nam P Nguyen, Thang N Dinh, Sindhura Tokala, and My T Thai. Overlapping communities in dynamic networks: their detection and mobile applications. In *Proceedings of the 17th annual international conference on Mobile computing and networking*, pages 85–96. ACM, 2011.

[20] Alessandro Mei, Giacomo Morabito, Paolo Santi, and Julinda Stefa. Social-aware stateless forwarding in pocket switched networks. In *Infocom, 2011 Proceedings Ieee*, pages 251–255. IEEE, 2011.

[21] Jérémie Leguay, Timur Friedman, and Vania Conan. Dtn routing in a mobility pattern space. In *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, pages 276–283. ACM, 2005.

[22] Jun-Won Ho, Matthew Wright, and Sajal K Das. Zonetrust: Fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing. *IEEE Transactions on Dependable and Secure Computing*, 9(4):494–511, 2012.

[23] Avinash Srinivasan, Feng Li, and Jie Wu. A novel cds-based reputation monitoring system for wireless sensor networks. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 364–369. IEEE, 2008.

[24] Tiejian Luo, Su Chen, Guandong Xu, and Jia Zhou. *Trust-based collective view prediction*. Springer, 2013.

[25] Yifei Wei, F Richard Yu, and Mei Song. Distributed optimal relay selection in wireless cooperative networks with finite-state markov channels. *IEEE Transactions on Vehicular Technology*, 59(5):2149–2158, 2010.

[26] Pan Hui, Jon Crowcroft, and Eiko Yoneki. Bubble rap: Social-based forwarding in delay tolerant networks, 2008.

[27] Orhan Dengiz. *Maximizing connectivity and performance in mobile ad hoc networks using mobile agents*. ProQuest, 2007.

[28] David Krackhardt. The ties that torture: Simmelian tie analysis in organizations. *Research in the Sociology of Organizations*, 16(1):183–210, 1999.

[29] Aminu Bello Usman, William Liu, Quan Bai, and Ajit Narayanan. Trust of the same: Rethinking trust and reputation management from a structural homophily perspective. *International Journal of Information Security and Privacy (IJISP)*, 9(2):13–30, 2015.

[30] Qing Ou, Ying-Di Jin, Tao Zhou, Bing-Hong Wang, and Bao-Qun Yin. Power-law strength-degree correlation from resource-allocation dynamics on weighted networks. *Physical Review E*, 75(2):021102, 2007.

[31] Aminu Bello, William Liu, Quan Bai, and Ajit Narayanan. Exploring the role of structural similarity in securing smart metering infrastructure. In *Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on*, pages 343–349. IEEE, 2015.

[32] Behrouz Jedari and Feng Xia. A survey on routing and data dissemination in opportunistic mobile social networks. *arXiv preprint arXiv:1311.0347*, 2013.

[33] Chiara Boldrini. Design and analysis of context-aware forwarding protocols for opportunistic networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*, MobiOpp '10, pages 201–202, New York, NY, USA, 2010. ACM.

[34] Aminu Bello Usman and Jairo Gutierrez. Trust-based analytical models for secure wireless sensor networks. In *Security and Privacy Management, Techniques, and Protocols*, pages 47–65. IGI Global, 2018.

[35] Aminu Bello Usman and Jairo Gutierrez. Datm: A dynamic attribute trust model for effcient collaborative routing. *Springer*, 2018.

[36] Feng Li, Jie Wu, and Anand Srinivasan. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In *INFOCOM 2009, IEEE*, pages 2428–2436. IEEE, 2009.

[37] Ari Keränen, Teemu Kärkkäinen, and Jörg Ott. Simulating mobility and dtns with the one. *Journal of Communications*, 5(2):92–105, 2010.

[38] Jouni Karvo and Jörg Ott. Time scales and delay-tolerant routing protocols. In *CHANTS '08: Proceedings of the third ACM workshop on Challenged networks*, pages 33–40, New York, NY, USA, 2008. ACM.

[39] Philo Juang, Hidekazu Oki, Yong Wang, Margaret Martonosi, Li Shiuan Peh, and Daniel Rubenstein. Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet. In *ACM Sigplan Notices*, volume 37, pages 96–107. ACM, 2002.

[40] Hoang Anh Nguyen, Silvia Giordano, and Alessandro Puiatti. Probabilistic routing protocol for intermittently connected mobile ad hoc network (propicman). In *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–6. IEEE, 2007.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500