A Decentralised Trust Framework for Emergency Communication using DTN

Philip Asuquo, Aneke Chikezie, Bliss Stephen
Department of Electrical/ Electronics & Computer Engineering
University of Uyo, Uyo
Akwa Ibom State, Nigeria

***Abstract*— This paper addresses mitigation of malicious behaviour in mobile and vehicular sensor networks under a mobility-aware scenario characterised by frequent disruptions. Delay Tolerant Networks (DTNs) are network architectures that have been developed to cope with intermittent connectivity in sensor networks. DTNs use an end-to-end message-oriented overlay called the bundle layer which is above the transport layer to help combat network interruption. In DTNs, malicious behaviour poses serious threats in forwarding messages from the source to the destination node. In this paper, we propose a mobility aware trust management scheme which utilises subjective logic to dynamically filter out misbehaving nodes in DTNs. We develop trust relationships from encounter record histories that have been exchanged by nodes to evaluate trustworthiness. We perform a comparative analysis of our proposed scheme with different mobility models against Encounter-Based Routing (EBR) which is a trust-based routing scheme and non-trust based (PROPHET and Spray-and-Wait) routing schemes. The results demonstrate that our scheme can deal with routing misbehaviour such as packet dropping attacks and outperforms EBR and the non-trust-based routing schemes without incurring high message overhead**.

I. I. INTRODUCTION

Delay/Disruption Tolerant Networks (DTNs) are networks developed to cope with intermittent connectivity and long delay in wireless networks. Unlike traditional networks where packets are forwarded along fixed links, DTNs use a store-and forward approach to overcome the lack of end-to-end paths [1]. DTNs comprise of nodes with limited resources such as buffer space and power, these resource constraints in addition to the sparsity and mobility of these nodes often result in intermittent connectivity. The application of DTNs spans across a wide range of applications including Under Water Networks (UWNs), Pocket Switched Networks (PSNs), Vehicular Ad-hoc Networks, Military applications and Disaster recovery and rescue operations [2], [3]. Mitigating routing misbehaviour using reputation and trust management schemes has been well studied in Wireless Networks [2]; however, there is no adequate attention to trust and reputation systems in DTNs. Although trust management and reputation-based strategies have been well studied in MANETS, the unique network characteristics of DTNs such as lack of end-to-end paths, unpredictable mobility patterns and long variable delays make these schemes unsuitable for DTNs [4]. Recent works in DTNs based on trust management show the challenges in message forwarding where routing misbehaviour from malicious nodes reduce the message delivery probability [4] – [9]. For instance, [10] evaluates the trustworthiness of a recommended node by using its encounter value. This trust recommendation may come from misbehaving nodes that collude with each other to degrade the network performance. Proposed trust management schemes are not adequately effective to filter out dishonest recommendations. Another proposed scheme [4] relies on a Trusted Authority (TA) to evaluate nodes behaviour which is costly in terms of transmission overhead and verification feedback. Additional security requirements will translate to more energy consumption which is a major challenge in DTNs. In mission-aware applications deployed using DTNs such as disaster recovery and rescue operations and tactical military warfare operations, DTNs must achieve their mission despite disruption or compromise of nodes.

To deal with these limitations, we propose a Mobility-Aware Trust Management Scheme (MATMS) for DTNs. We focus on mobility-aware models that capture some degree of recurrence in modelled activities such as the Post Disaster Model (PDM) [3]. Nodes maintain a set of neighbours that they encounter recurrently. We develop a trust relationship from the intercontact graph formed from the encounter records. Compared to the approaches in [4]–[9] which rely on direct and indirect encounters to formulate trust, we develop a novel approach using subjective logic. Consensus and discounting approaches from subjective logic are used to formulate trust networks. The consensus approach deals with self-promoting attacks while the discounting approach deals with colluding attacks.

The main goal of our approach is to increase delivery ratio and reduce message delay in mobility-aware DTNs. We combine opinion splitting from trust network and latency distributions from the inter-contact graph to provide QoS in making forwarding decisions. The MATMS simplifies trust graph into series-parallel graph by the removal of uncertain paths to obtain a canonical graph. Trust transitivity means that if node *i* trust node *j* which trust *k*, then node *i* will trust *k* which is achievable through indirect trust from node *k* to *i* as illustrated in Fig.1. Trust is a dynamic property in DTNs as a result of the changing network topology. In our proposed scheme, trust is aggregated along with uncertainty which makes the aggregated value more reliable than other approaches. Trust is incorporated into the routing decision to protect against packet malicious misbehaviour such as dropping attacks.

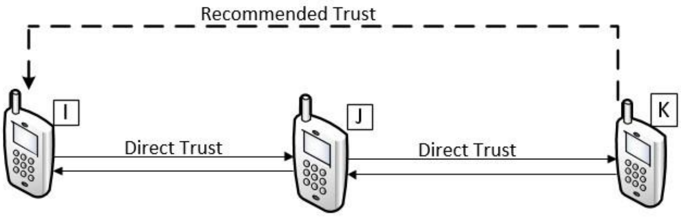

Fig. 1: Transitive trust principle

We use subjective logic [11] which is suitable for the analysis of networks as trust relationships can be expressed as opinions with degree of uncertainties. To establish trust using subjective logic, we express binomial opinions as trust and map them into Probability Density Function (PDF). A belief system is developed to evaluate the trustworthiness of a forwarding node based on the inter-contact graphs. This belief which is expressed as opinions will not only reflect a node's trustworthiness towards another node but will also reflect the to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.

belief of the prediction through the measured uncertainty. The trust opinion formed from these nodes as they come in contact with each other are used to make forwarding decisions.

To validate our proposed scheme, we implement extensive simulations in ONE [12] simulator to reflect mission critical scenarios using the Post Disaster Model (PDM) [3] - RFC 7576 [13] which is a reference model for emergency support and disaster recovery and compare the performance of our proposed scheme with existing benchmarks schemes when nodes are compromised. Simulation results show that MATMS mitigates routing misbehaviour without incurring high message cost under best trust formation.

The rest of the paper is organised as follows. We discuss related work in Section II. The network scenario, attack model and design goals are presented in III. In Section IV, we introduce some background work on subjective logic and present our proposed scheme. We carry out a performance evaluation in Section V to evaluate the performance of our proposed scheme and conclude our work in Section VI.

II. II. RELATED WORK

In this section, we discuss the existing trust and reputation management schemes in Peer-to-Peer (P2P) and WSNs, Mobile Ad-hoc, and trust management schemes in DTNs.

A. *Trust Management in P2P and WSNs*

In the context of P2P networks, trust management schemes are distributed; there is no central authority to monitor and evaluate the trustworthiness of nodes in the network. Each node monitors and evaluates the trustworthiness of its neighbouring nodes. In structured P2P networks, a decentralised trust management scheme which uses a P2P look up system based on a search tree that is virtually distributed is proposed by [14]. Each peer is assumed to be a trustworthy neighbour unless a complaint is received by the virtually distributed tree search. The authors in [15] propose Eigen Trust, a secure and distributed strategy to compute global trust values based on iteration. This global trust is computed using transitivity and stored in a Content Addressable Network (CAN). Similar to the approach in [15], a decentralised reputation-based trust supporting framework (Peer Trust) with an adaptive trust model for evaluating the trustworthiness of peers based on a transactional feedback system is proposed by [16]. Both Eigen Trust and Peer Trust use the trustworthiness of the recommender to evaluate the indirect trust. The authors in [17] propose a new fair scheduling technique Power Trust to leverage the power law feedback characteristics. This robust and scalable P2P reputation system uses a distributed ranking mechanism to dynamically select nodes that are most reputable in a P2P network. In unstructured P2P, the trust queries are generally flooded to the network. A detailed model for trust computation is not defined in the model as presented in [18]–[21]. Peers use collective feedback in decision making to mitigate inauthentic file downlands.

including packet drop rate, control packets and data packets. Each node stores these weighing mechanism in a trust table and sends feedback to the selected cluster heads. In event-driven WSNs, authors in [25] propose a reputation-based protocol (TIBFIT) to diagnose and mask arbitrary node failures. This protocol analyses the binary reports from neighbours to determine the occurrence of an event. An active detection-based security (ActiveTrust) and trust scheme is proposed for WSNs by [26]. This trust-based routing scheme uses the trust level of neighbouring nodes and the trust requirements of a packet to select an optimal forwarding path. ActiveTrust creates detection routes to compute nodal trust thereby preventing blackhole attacks and optimizing the lifetime of the network. An integrated trust management framework (iTrust) is proposed in [27] to evaluate the trustworthiness of nodes in the neighbourhood using monitor nodes. These special nodes gather information about neighbouring nodes and share their trust indices with encountered nodes which is used to make forwarding decisions.

B. *B. Trust Management in Ad-Hoc Networks*

In ad-hoc networks, several schemes have been proposed and discussed in a comprehensive survey by [28]. A recommendation-based trust model with a defence scheme has been proposed to filter trust propagation attacks using clustering techniques [29]. This scheme pays attention to attacks that are related to dishonest recommended from neighbouring nodes in a particular time frame based on the number of encounters. To measure and model trust evolution, an information theoretic framework is proposed in [30] using entropy and probability to acquire, maintain and update trust behaviour that are associated with the behaviour of nodes. In the proposed framework, propositions are developed to establish trust through third parties, assist in route selection and malicious node detection. In [31] authors extend the notion of traditional trust to datacentric framework for the establishment of trust based on several evidence techniques. They pay attention to networked systems that are highly volatile and resource constrained and use the theory of Dempster-Shafer to evaluate data reports and compare their results to weighted and Bayesian schemes. In [32], a fully distributed public key certificate management based on trust graph and cryptographic threshold is proposed. In this model, users can issue public key certificates and also perform authentication using the certificates. The threshold cryptography is used to check misbehaving nodes that issue false public key certificates.

C. *Trust Management in DTNs*

To maximise delivery ratio and reduce the transmission cost of messages, an Encounter Based Routing (EBR) [10] has been proposed to evaluate the trustworthiness of a node when it encounters another node. This routing strategy uses an encounter value (EV) which is a reputation metric obtained from a current window counter forwarding evidences. EBR has been widely adopted for DTN routing as most research works in DTNs leverage on its routing strategy. In [6], a novel methodology is proposed to deal with malicious and selfish behaviour. This trust management protocol which incorporates QoS is based on Stochastic Petri Net (SPN) and is designed to optimise the routing performance in DTNs. Extensive simulation analysis has shown that the proposed scheme outperforms Bayesian trust routing schemes, Epidermic and PROPHET routing protocols with a lower message overhead. Similarly, authors in [33] propose a Provenance based trust model (PROVEST) for accurate peer to peer assessments. In this model, a data driven strategy is used to reduce the consumption of constrained resources. The authors in [5] propose a graph-based iterative algorithm as a robust trust mechanism for node detection. In a comparative analysis using extensive simulations, authors have illustrated that their proposed scheme performs better than other trust management schemes such as the Eigen Trust and Bayesian framework [15] under Byzantine attacks. A Probabilistic Misbehaviour Detection Scheme (PMDS) has been proposed by [4] based on data forwarding evidences. In this scheme, the inspection game in [34] is adopted to demonstrate the cost of misbehaviour detection. Simulation results show that there is a reduction in the forwarding cost that is incurred by iTrust and that iTrust effectively detects routing misbehaviour by the malicious nodes in both single and multi-copy routing protocols in DTNs. To reduce the detection time and improve precision, a Collaborative Contact-based Watchdog (CoCoWa) which is based on a local watchdog detection is proposed in [35]. When a node encounters another node, a diffusion module is used to transmit and process false positives and negatives. Analytical and experimental results presented using the proposed scheme show that the detection time in reduced as well the message transmission cost when nodes collaborate using the diffusion module.

encounter with node, it may assume the encountered node is malicious. In ad hoc networks, trust degrades automatically as the number of hop increases. This may not be true in DTNs as node rely on a hop-by-hop forwarding approach. Filtering out malicious nodes that propagate false recommendations has not been effectively tackled in MANETs. These nodes collude with each other and exaggerate trust rating across the network. In DTNs, trust management schemes proposed focus on selfish behaviour. Most schemes use mobility models such as Random Way Point (RWP) which is inadequate to model trust relationship from transitivity. Game theoretic models such as iTrust effectively detects misbehaving nodes but very NETWORK SCENARIO, ATTACK MODEL AND DESIGN GOALS

D. *A. Network Scenario*

We consider DTNs deployed in mission-aware scenario. We adopt the Post Disaster Model (PDM) proposed by [3] and recommended by IETF (RFC 7476) as a baseline scenario for disaster recovery operations [36]. We assume that the disaster scenario consists of a group of nodes deployed in an open and hostile environment such as the Great East Earthquake in Japan, 2011 where over 375 base stations were destroyed, over 90 routes were disconnected from the relay transmission lines and the traditional telecommunication services were unavailable [37].

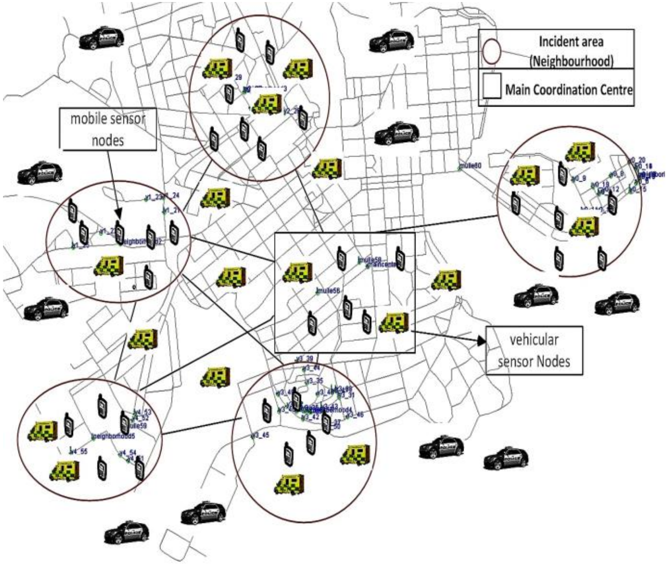

Fig. 2: Illustration of Scenario

In this scenario, we consider a community of interest where there is a DTN with several wireless devices (i.e nodes) moving in a community which are either held by people or fixed on vehicles (Data Mules). This scenario is based on the PDM in ONE shown in Fig. 2. Nodes move from one sub-task to another as needs arise during mission executions, a node can also move around multiple sub-task groups if it is assigned to multiple sub-task events described in the movement models such as between centre movements which is the movement between the coordination centres which include; the relief camps, evacuation centres, medical centres and the police and fire stations. Other mobility patterns undertaken by these responder nodes include; event driven, cyclic route and convergence move.

To protect a network from a wide range of attacks, traditional security mechanisms are not robust enough especially with networks that lack end-to-end connectivity and a predefined network architecture. In DTNs, malicious nodes aim to break routing capabilities in addition to dropping packets and exhibiting selfish behaviours. A malicious node can be an internal attacker with the aim of disrupting the operation of a mission such as disaster recovery operations and in tactical warfare scenarios. When two nodes meet, an encounter

record is generated. Assuming node *i* comes in contact with node *j*, an encounter record ER_i is generated as shown below:
Definition 1. An interaction ER^i_j between two nodes can be expressed as follows:

$$ER^i_j = [N_i, N_j, N_{dst}, FL_i, RL_i, Ts, T_{mexp}]$$

where N_i, N_j, N_{dst} are node identifiers for node *i*, *j* and the destination node. FL_i and RL_i represent the list of messages forwarded and received by node *i*. T_s is the time stamp while T_{mexp} is the expiration time of the message. Due to the resource constraints, a node keeps its most recent ER to reduce computational overhead
.

B. Attack Model

In mission critical or situation specific scenarios like tactical and post disaster communication networks using DTNs, malicious nodes can launch an attack by dropping packets forwarded to them. An attacker first receives a packet relayed to it then, it drops them with a certain probability which can lead to serious performance degradation. Malicious nodes can drop packets forwarded to them even if they have enough buffer space to store these messages.

1) Self-Promoting: Malicious nodes manipulate their own trustworthiness; this can be done by falsely increasing their probability of expectation. The main purpose of this attack is to attract packets and drop them later.

2) Time-dependent attacks: Honest nodes can start misbehaving after a time interval, this malicious behaviour can provide false recommendations at different time intervals which will lead to the malfunctioning of the whole trust management framework.

3) Bad-mouthing attacks: Providing bad recommendations to tarnish the reputation of well-behaved nodes may lead to a decrease in their chances of relaying packets across the network. Such fraudulent behaviour prevents nodes from relaying packets using the best routes in the networks. Trusted nodes can conspire to propagate these unfavourable rating of healthy nodes.

4) Ballot-stuffing attacks: This attack is aims at misleading the trust management framework. Providing compromised nodes with good reputation based will result in over exaggeration of the reputation of nodes. This attack increases the chances of relaying packets through malicious nodes so that they can drop or temper with packets relayed to them.

III. PROPOSED FRAMEWORK

The trust computation is based on the history of encounters known as the Encounter Record (*ER*). Suppose two nodes *i* and *j* come in contact with each other, *ER* generated by node *i* about node *j* is denoted by $ER^i_j = (ER_1, ER_2, ...ER_n)$ where ER_1 is a single interaction record with node *j*. We describe how trust can be derived with the belief of subjective logic which uses opinion as a belief metric. We briefly describe the process of deriving trust from nodes interaction to form ERs. The stored ERs are used to form the trust relationship. This relationship is later converted into trust opinions ω. To quantify the trust value associated with the encountered node, the trust paths from the trust network is evaluated. Subjective logic operators (⊕, ⊗) are applied to the trust paths to obtain a quantifiable trust value E(ω). The latency distribution of the transitive paths is evaluated and the path with least average delay is selected as next message hop.

A. Subjective Logic

Subjective logic [11] can be described as a belief calculus which allows nodes to express their opinions about propositions as degrees of belief, disbelief and uncertainty. Subjective logic is suitable for the analysis of trust networks as trust relationships can be expressed as opinions with degrees of uncertainties to monitor the behaviour of encountered and neighbouring nodes in the community of interest. To establish trust using subjective logic, we express binomial opinions as trust ω = (*B*, *D*, *U*) where (*B*, *D*, *U*) represent belief, disbelief and uncertainty. With accumulated forwarding evidences from encounter records, malicious nodes may provide compromised computed trust values. These trust values do not reflect the node’s behaviour if each record is treated equally regardless of time of encounter. In subjective logic, the notion of opinion can be expressed as a belief built on trust. We adopt [11] which uses trust transitivity to compute trust along a chain of trust edges. for example, two nodes *i* and *j* where *i*’s opinion towards *j* is denoted by ω^i_j which is the trust worthiness of *j* towards *i* can be described as on opinion vector.

Definition 2. An opinion ω is denoted by an ordered triplet, (*B*, *D*, *U*) such that $B + D + U = 1$ where $B, D, U \in [0, 1]$ and *B*, *D*, *U* represent belief, disbelief and uncertainty.

Definition 3. (Consensus Opinion) Let *i*, *j* and *k* be three DTN-nodes, then $\omega^i_k = [B^i_k, D^i_k, U^i_k]$ and $\omega^j_k = [B^j_k, D^j_k, U^j_k]$ be opinions respectively held by node *i* and *j* about the trustworthiness of node *k*. The consensus trust can be defined as $\omega^{ij}_k= \omega^i_k \oplus \omega^j_k$ which is the combined opinion between ω^i_k and ω^j_k. The symbol ⊕ is used to designate the consensus operator.

$$\omega^{ij}_k = B^{ij}_k, D^{ij}_k, U^{ij}_k \qquad (1)$$

The consensus opinion which is equivalent to Bayesian updating in statistics reflects conflicting opinions in an equal and fair strategy. Nodes *i* and *j* have opinions about the trustworthiness of an encountered node *k* from distinctive *ER* about node *k*. Combined opinions help in the reduction of uncertainty. The consensus opinion is an aggregated opinion from node *i*, *j* and *k*.

Definition 4. (Opinion Discounting) Let $\omega^i_j = [B^i_j, D^i_j, U_j^i]$ represent the opinion of node *i* towards *j* and $\omega^i_j = [B_k^j, D_k^j, U_k^j]$ represent node *j*’s opinion towards *k*. Node *i* will take the recommendation of node *j* toward *k* as:
Opinion discounting which is denoted by a discounting operator ⊗ is used to compute trust along a transitive path [11]. It shows how node *i* computes the indirect trust given by the knowledge of node *j* about *k*. Opinion discounting is derived from the discounting function by [38] using a discounting rate. Node *i*’s belief in the opinion of *j* becomes the uncertainty towards node *k* rather than its disbelief and node *i*’s uncertainty in *j* also becomes part of the uncertainty in node *k*.

Definition 5. The probability expectation value of a binomial opinion T_{ij} is expressed as:

$$E(\omega^{i}_{j}) = B^{i}_{j} + aU_{j}^{i} \qquad (2)$$

where B^{i}_{j}, U_{j}^{i}, a represent the belief, uncertainty and base rate as described in [11]. The expression in Eq. 2 is equivalent to the pignistic probability [39] in decision theory. In [39], belief can be used to make decisions and these decisions are quantified by probability functions. In the context of trust computation, ω^{i}_{j} can be expressed as a trust opinion of node *i* on *j*. The value of ω^{i}_{j} given in Eq. 2 represents the predicted value of the trust opinion ω^{i}_{j} as a quantifiable value.

A. *B. Conversion of Trust Relationship*

In general terms, a set of previous encounters is used to formulate the trust between two nodes. We describe this trust relationship with the following definition.

Definition 6. The trust relationship T_{j}^{i} between two nodes is given as:

$$T_{j}^{i} = [ER_{n}, a, s, f, ER_{w}] \qquad (3)$$

where T_{j}^{i} denotes node *i*'s trust in relation to node *j*, ER_{n} is the total number of interactions between nodes *i* and *j*, *a* is the base rate which is the prior probability in the absence of belief and disbelief, *s*, *f* represents positive and negative events from previous encounters and the ER_{w} represents the window size of the ERs. To convert trust relationship T_{j}^{i} into an opinion ω^{i}_{j}, the probability density is expressed over binary events as a Beta Probability Density Function (PDF). Beta distribution is a family of continuous probabilities denoted by (α, β) on the interval [0,1]. Let *s*, *f* represent the number of positive and negative observations from the interactions between nodes *i* and *j*, the Beta (PDF) can be expressed as:

$$\alpha = s + 2a \qquad \text{and} \qquad \beta = f + 2(1 - a) \quad (4)$$

where *s* and *f* represent positive and negative observations and *a* is the base rate. Adopting the approach in [11], we bijectively map between the opinion parameters and Beta (PDF).

C. Formulation of Trust Relationship with Trust Transitive Paths

In DTN, a trust network can be conceptualised as a directed graph from the aggregation of individual trust relationships. The analysis of trust propagation is based on the notion of transitivity: Trust transitivity means that if node *i* trusts node *j* which trusts node *l*, then node *i* will also trust node *l*.

There is a possibility of getting two or more cyclic paths cyclic paths. We consider a minimal path solution so that the number of transitive hops in the trust network is minimised. To represent trust transitive networks as directed graphs, we add some elements of notation to enable us express trust networks in a structured way as shown in Eq.8. We introduce an edge splitting approach so that each node is connected to an independent edge and $T_{n}[i, l]$ is expressed as;

$$\begin{aligned} T_{n}[i, l] &= ([i, j] : [j, l]) = [M_{1} : M_{4}] \qquad (5) \\ &= ([i, k] : [k, l]) = [M_{2} : M_{5}] \end{aligned}$$

D. Trust Evaluation

The final stage of establishing trust between nodes is to compute the trust value of each node based on the trust relationship established from Definition 3 and 4 which are applied to the edges that link the transitive path between the source and destination nodes. The trust relationship is expressed as a quantifiable trust value which is the probability of expectation $E(\omega)$ defined in Eq. 3. In summary, a node's trust inference system is developed by collecting and aggregating forwarding evidences from previous encounters, then it builds and stores the trust relationship and develops an assessment procedure for evaluating the trust value. A node's trust level is defined as a real number in the range of [0, 1]

E. Message Forwarding Scheme Description

The primary goal of every DTN message forwarding protocol is to obtain a high message delivery ratio and good latency performance. Widely adopted message forwarding schemes such as MaxProp and RAPID achieve high delivery ratios with excessive consumption of limited network resources while quota-based protocols such as Spray and Wait, Spray and Focus that have low message overhead are not able to achieve comparable message delivery ratios [2]. In traditional wireless networks, latency depends on the condition of the egress links, packets remain in the buffer till the link becomes available. Latency in DTNs is quite different because the latency of a packet depends not only on the next hop but previously encountered node.

We use the inter-contact graph between two edges to calculate the latency between two encounters. We use the notation $M_{1} \rightarrow M_{2}$ to denote a directed edge between two nodes that come in contact. Each edge is maintained by a finite order list of elements (2 tuples) $\rho(ij \rightarrow ik)$ which is the average latency elapsed from node *i* from an encounter with node *j* and *k*. We use edge splitting to produce independent paths to calculate the path latency as shown in Fig. 4, we compute the path latency as $\rho(ij \rightarrow l) = M_{1}$, $\rho(ik \rightarrow l) = M_{2}$ so that the entry for destination node *l* has corresponding path latency of $(ij \rightarrow l)$ and $(ik \rightarrow l)$ as a parametric summary of latency distribution for node *i* to make its forwarding decisions. It is important for a source node to have an idea of the latency distributions to enable it make realistic estimations of the probability of successful deliveries to the destination nodes

1) Routing Decision: In mission-aware scenarios where the movement models have similar or recurring traffic patterns such as the movement between emergency centres in a disaster network captured in the PDM model [3] and ETSI reference model for Emergency recovery and disaster relief operations [36]. It is important to achieve an effective forwarding strategy so that relayed messages use the optimal routing path for to make forwarding decisions. In our proposed scheme, we do not only consider the trustworthiness of a node before making a forwarding decision. We pay attention to latency distributions formed from the interconnect graph from source node to the destination node.

The proposed scheme concurrently considers the latency of each independent path and the trust metric from the probability of expectation in Eq. 3. Assuming node *i* encounters nodes *j* and *k*, node *i* can choose between nodes *j* or *k* as the next hop to relay its message to *l* based on the following steps: node *i* exchanges its *ER* table with node *j* and *k*, there is a feedback mechanism for acknowledgement for each encounter. To evaluate the trustworthiness of an encountered node, the two nodes exchange their trust table and update their ERs. After the trust updates, node *i* will determine whether to forward the packets to nodes *j* or *k* based on the trust value and latency distribution from (*i* → *l*). This is a Quality of Service (QoS) measurement which enables messages to be forwarded using the optimal route. However, the trust values take precedence over the latency distributions.

2) ER Aging in MATMS: To provide resiliency, we use an *ER* window ER_w to check for collaborative attacks. A malicious node can exhibit a certain behaviour such as starting up as a trustworthy node but later becomes a malicious node. This behaviour makes the forwarding evidences collected before the node's change of nature misleading. To alleviate this problem, we create a window size where old assessments are discarded in a process known as *ER* aging. For every encounter, there is a T_{ts} which is used in in the assessment of the *ERs* for a particular ER_w. Assuming node *j* starts misbehaving at time T_{25}(mins) and the periodic rate of the ER_w is T_{600}(mins). If the prior forwarding evidences from node *j* is large, it will take a long time for its neighbouring nodes to find out about the change in its behaviour.

IV. PERFORMANCE EVALUATION

A. A. Simulation Setup

This simulation is implemented in ONE simulator for DTN protocol evaluation [12]. We simulate MATMS on top of the PDM model, Random Way Point and Shortest Path Map Based mobility model. The PDM model was developed by [3] and recommended by IETF [36] for Information Centric Networks: Baseline Scenarios for Emergency Support and Disaster Recovery operations. The Map-Based mobility model constrains the movement of nodes the paths defined in the map data. The arbitrary map data defined in Well Known Text (WKT) is understood by the movement models in the PDM which are created using OpenJump, a Geographic Information System (GIS) program for converting real-world map data. We use five neighborhoods, 4 main centres, 10 relief and evacuation camps, 100 rescue workers, 10 supply vehicles, 10 emergency vehicles, 10 police patrols for the PDM simulation setup which runs for 48 hours. We use a simulation area of 4,500 × 3,400 m, at speeds of 0.5−1.5 km/h for pedestrians and 2.7−13.9 km/h for vehicles. For each of these scenarios, data traffic is generated as a Poisson's process at the rate of one message per 5 minutes for a randomly selected source destination pair similar to message generation adopted by [3]. Similar to the approaches in [6], [40], each node has a buffer size of 50 MB and the message size is in the range of 50kB 5MB. For each experiment, the simulation runs for 10 times with random seeds and the average of the metrics measured are presented.
We use the same simulation setting to evaluate the performance of MATMS for Shortest Path Map-based Movement and Random Way Point (RWP) mobility models.

- Shortest Path Map-based Movement Model: This mobility model constraints the movement of nodes to predefined paths. Different paths can be defined for a specific group or all the nodes in the network.
- Random Waypoint (RWP): RWP is a synthetic movement model. It is a movement model where nodes randomly select their speed and destinations. In RWP, it is difficult to model a realistic statistical distribution of events. This is because RWP is an abstract movement model and does not capture realistic mobility patterns.

We also conduct a comparative analysis comparing our proposed scheme to Encounter Based Routing (EBR) scheme. EBR uses an encounter-based metric which maximizes message delivery ratio while minimizing overhead both in terms of extra traffic injected into the network and control overhead [10]. In addition to the EBR protocol, we evaluate MATMS against two other routing protocols: PROPHET [41] and Binary Spray and Wait [42]. PROPHET uses history of encounters and transitivity to compute the probability of message delivery by a node while Spray and Wait sprays a limited number of copies (L = 6) into the network, and then waits till one of these nodes meets the destination node.

B. B. Performance of MATMS

In this section, we consider the efficiency metrics and general performance that apply to many routing protocols, We focus on three performance metrics in DTNs: message delivery ratio, message latency and message overhead. These metrics used in evaluation are described as follows;

- Delivery Ratio: This is the percentage of messages delivered to the total number of messages created.
- Latency: The latency is computed as the average period of time that a message needs to travel from the source node to the destination node.
- Overhead ratio: This is the ratio of the total number of messages relayed to the total number of messages delivered.

In Fig. 4 (a) delivery ratio, (b) overhead ratio and (c) latency, we explore the performance of MATMS with different traffic patterns in the PDM. In an emergency response network, the performance varies based on movement patterns. We evaluate the impact of malicious responders on these traffic patterns: rescuers-to-rescuers (R-R), messages relayed by responders among themselves for the disaster recovery operation), Patrol (Police Patrol and fire trucks), centre-to-centre (C-C) between centre movements similar traffic patterns are also captured in the ETSI reference model for disaster recovery and rescue operations [43] such as movement between Casualty Collection Point (CCP) and Temporary Care Centre (TCC). In Fig 4, we show that under our best trust formation with percentage of malicious nodes varying from [0-50 percent], the delivery ratio remains high even with 50 percent of malicious responder. The latency and overhead also decrease as the number of malicious nodes increase because only trusted responder nodes take part in message forwarding hence the path cost and delay have reduced and these metrics are calculated from source to destination nodes.

C. C. Comparison with other Schemes Proposed

In Fig. 6, we present the performance evaluation results of MATMS alongside other routing protocols on the Post Disaster Mobility mode (PDM). It is observed that the map-based mobility model enhances delivery ratio for all routing schemes. This is as a result of the mobility pattern which yields more encounter opportunities, role-based and event driven models capture distinct movement patterns hence they can achieve higher delivery ratio. Our simulation results in Fig. 5 shows the impacts of malicious nodes on the network in different mobility model. We observe that our proposed scheme (MATMS) and the EBR scheme have less performance degradation in delivery ratio when compared PROPHET and Spray and Wait. This is because messages are forwarded to relay nodes based on trust and relay nodes must be trustworthy before a message is relayed to them. Our scheme outperforms EBR and the other routing schemes when considering message delivery. In Fig 5 (b), we analyse the impacts of the malicious nodes on message overhead for the different movement models, we observe that our trust-based scheme is significantly lower than EBR and the other routing schemes even with malicious nodes. Again, we analyse the impacts of malicious nodes on the message delay in the post disaster model in Fig 5 (c). We observe that when the percentage of malicious nodes increase, the latency decreases because messages are forwarded to only trusted nodes and dropped messages are not considered in calculating the message latency. We can see that our scheme which incorporates a node's latency distribution to make forwarding decisions outperforms the other routing schemes.

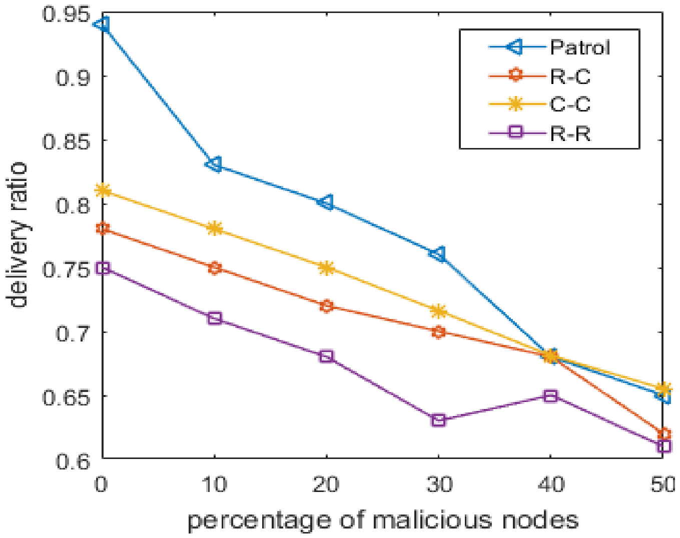

Fig. 4a: Delivery ratio of MATMS in various traffic patterns in the PDM

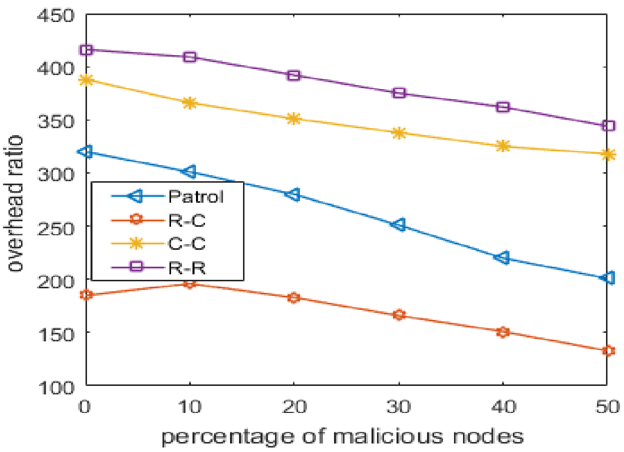

Fig. 4b: Overhead ratio of MATMS in various traffic patterns in the PDM

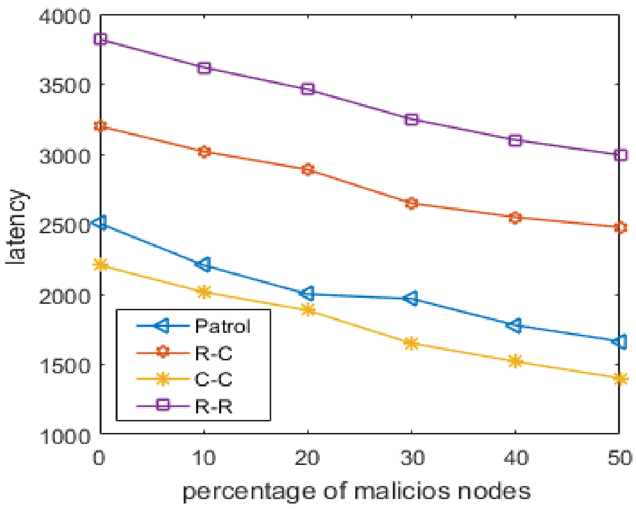

Fig. 4c: Latency of MATMS in various traffic patterns in the PDM

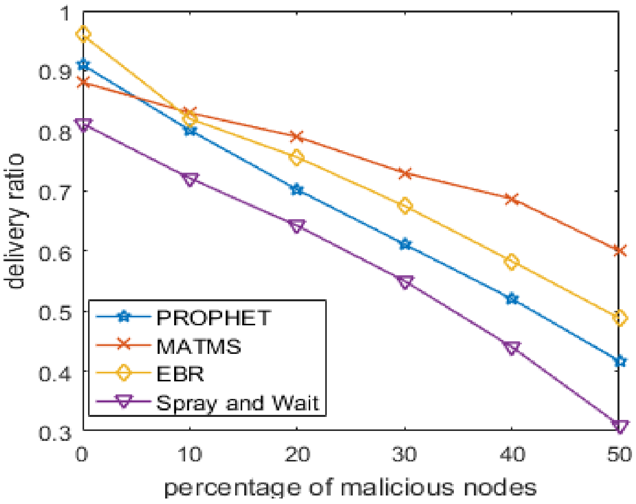

Fig 5(a) Comparison ofMATMS delivery ratio with other approaches

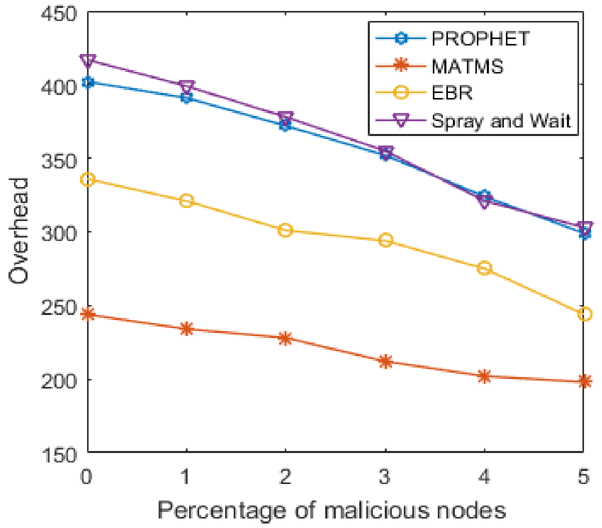

Fig 5(b) Comparison of MATMS overhead ratio with other approaches

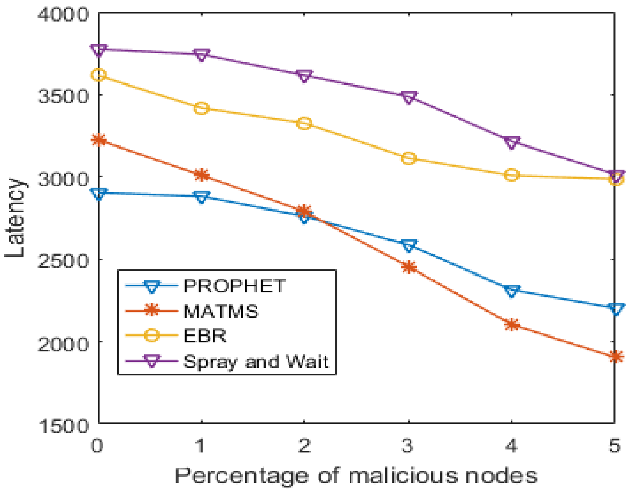

Fig 5(c) Comparison of Latency of MATMS with other approaches

Mitigation Efficiency with Aging ER: In resource constrained networks, nodes may have limitations in their storage capabilities which may affect the no of records kept by a node for an ER_W. We evaluate the performance of MATMS and EBR with different ER_w sizes. We consider collaborative attacks with a dropping probability of 0.6 under the same simulation setting described in Section V-A. In Fig. 6 (a) and (b), we show the false positive and the detection accuracy over a varying ER_w. Our results show that a larger ER_w size achieves a higher detection accuracy while reducing the false positive rate. The results also show that the detection performance of MATMS under varying ER_w sizes outperforms EBR. This implies that nodes with limited storage will have a lower detection accuracy and higher false positive ratio when compared to nodes with lower ER_w.

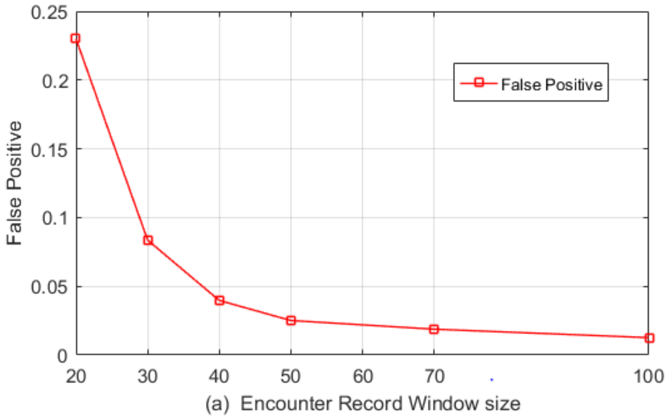

Fig. 6(a) Mitigation Efficiency under varying window size for False Positives

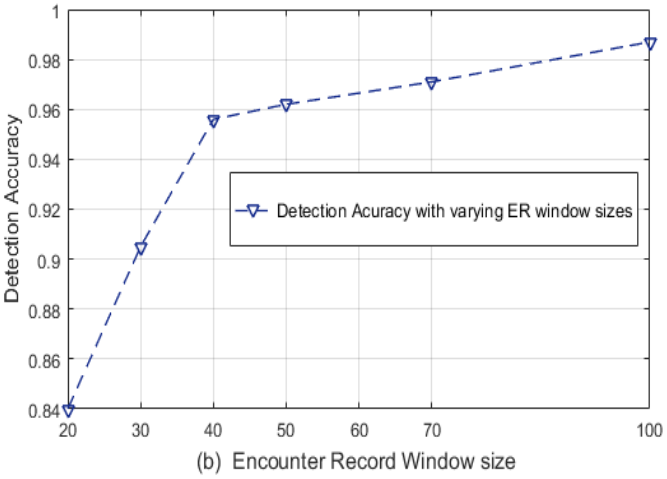

Fig. 6(b) Mitigation Efficiency under varying window size for Detection Accuracy

V. CONCLUSION

The opinion logic is a core dimension of trust which reflects the confidence in the adequacy of a node's previous interactions. Malicious activities from compromised nodes can lead to uncertainty in the forwarding behaviour of nodes thereby degrading the network. Thus, it is necessary design and implement appropriate packet forwarding strategies to address this misbehaviour in DTNs. In this paper, we present a mobility-aware trust management scheme based on subjective logic to compute trust between two nodes for data forwarding in DTNs where malicious nodes attempt to degrade the network performance by malicious behaviour. We exploit the mobility properties of the PDM to improve cooperation and reduce uncertainty. The proposed scheme outperforms other routing protocols by providing a higher delivery ratio while reducing overhead ratio and delivery delay. Our results also confirm that binomial Dirichlet distribution can be exploited to improve node cooperation in resource constrained networks.

VI. REFERENCES

[1] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme in DTN," in *2012 IEEE International Conference on Communications (ICC)*, pp. 4970–4974, June 2012.

[2] Y. Cao and Z. Sun, "Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 654–677, 2013.

[3] M. Uddin, D. Nicol, T. Abdelzaher, and R. Kravets, "A post-disaster mobility model for Delay Tolerant Networking," in *Simulation Conference (WSC), Proceedings of the 2009 Winter*, pp. 2785–2796, Dec. 2009.

[4] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in DelayTolerant Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 22–32, Jan. 2014.

[5] E. Ayday and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 1514–1531, Sept. 2012.

[6] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, “Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 1200–1210, May 2014.

[7] B. Chen and M. C. Chan, “MobiCent: a Credit-Based Incentive System for Disruption Tolerant Network,” in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, Mar. 2010.

[8] F. Li, J. Wu, and A. Srinivasan, “Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets,” in *IEEE INFOCOM 2009*, pp. 2428–2436, Apr. 2009.

[9] Y. Wang, M.-C. Chuah, and Y. Chen, “Incentive Based Data Sharing in Delay Tolerant Mobile Networks,” *IEEE Transactions on Wireless Communications*, vol. 13, pp. 370–381, Jan. 2014.

[10] S. Nelson, M. Bakht, and R. Kravets, “Encounter-Based Routing in DTNs,” in *IEEE INFOCOM 2009*, pp. 846–854, Apr. 2009.

[11] A. Jøsang and T. Bhuiyan, “Optimal trust network analysis with subjective logic,” in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, pp. 179–184, Aug 2008.

[12] A. Keränen, J. Ott, and T. Kärkkäinen, “The ONE Simulator for DTN Protocol Evaluation,” in *SIMUTools ’09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, (New York, NY, USA), ICST, 2009.

[13] E. Davies, G. Tyson, B. Ohlman, S. Eum, A. Molinaro, D. Corujo, K. Pentikousis, and G. Boggia, “Information-centric Networking: Baseline Scenarios,” IETF Draft Version 3 RFC 7476, IETF, February February 2015.

[14] K. Aberer and Z. Despotovic, “Managing trust in a peer-2-peer information system,” in *Proceedings of the Tenth International Conference on Information and Knowledge Management*, CIKM ’01, (New York, NY, USA), pp. 310–317, ACM, 2001.

[15] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The eigentrust algorithm for reputation management in p2p networks,” in *Proceedings of the 12th International Conference on World Wide Web*, WWW ’03, (New York, NY, USA), pp. 640–651, ACM, 2003.

[16] L. Xiong and L. Liu, “Peertrust: supporting reputation-based trust for peer-to-peer electronic communities,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, pp. 843–857, July 2004.

[17] R. Zhou and K. Hwang, “Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing,” April 2007.

[18] B. Yu, M. P. Singh, and K. Sycara, “Developing trust in large-scale peer-to-peer systems,” in *Multi-Agent Security and Survivability, 2004 IEEE First Symposium on*, pp. 1–10, Aug 2004.

[19] B. Yu, M. P. Singh, and K. Sycara, “Developing trust in large-scale peer-to-peer systems,” in *IEEE First Symposium onMulti-Agent Security and Survivability, 2004*, pp. 1–10, Aug 2004.

[20] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, “Randomized gossip algorithms,” *IEEE Transactions on Information Theory*, vol. 52, pp. 2508– 2530, June 2006.

[21] R. Zhou, K. Hwang, and M. Cai, “Gossiptrust for fast reputation aggregation in peer-to-peer networks,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, pp. 1282–1295, Sept 2008.

[22] M. B. S. Saurabh Ganeriwal, Laura K. Balzano, “Reputation-based framework for high integrity sensor networks,” *ACM Trans. Sen. Netw.*, 2005.

[23] Z. Yao, D. Kim, and Y. Doh, “Plus: Parameterized and localized trust management scheme for sensor networks security,” in *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 437– 446, Oct 2006.

[24] G. V. Crosby, N. Pissinou, and J. Gadze, “A framework for trustbased cluster head election in wireless sensor networks,” in *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pp. 10 pp.–22, April 2006.

[25] M. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. C. Hu, “Tibfit: trust index based fault tolerance for arbitrary data faults in sensor networks,” in *2005 International Conference on Dependable Systems and Networks (DSN’05)*, pp. 672–681, June 2005.

[26] Y. Liu, M. Dong, K. Ota, and A. Liu, “Activetrust: Secure and trustable routing in wireless sensor networks,” Sept 2016.

[27] K. Yadav and A. Srinivasan, “itrust: An integrated trust framework for wireless sensor networks,” in *Proceedings of the 2010 ACM Symposium on Applied Computing*, SAC ’10, (New York, NY, USA), pp. 1466–1471, ACM, 2010.

[28] M. Momani and S. Challa, “Survey of trust models in different network domains,” *CoRR*, vol. abs/1010.0168, 2010.

[29] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, “Recommendation based trust model with an effective defence scheme for manets,” *IEEE Transactions on Mobile Computing*, vol. 14, pp. 2101–2115, Oct 2015.

[30] Y. L. Sun, W. Yu, Z. Han, and K. J. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks,” *IEEE J.Sel. A. Commun.*, vol. 24, pp. 305–317, Sept. 2006.

[31] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, “On datacentric trust establishment in ephemeral ad hoc networks,” in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008.

[32] M. Omar, Y. Challal, and A. Bouabdallah, “Reliable and fully distributed trust model for mobile ad hoc networks,” *Journal of Compuers and Security*, vol. Volume 28, Issues 3U4,, p. Pages 199″ U214, May-June″ 2009 2009.

[33] J. H. Cho and I. R. Chen, “Provest: Provenance-based trust model for delay tolerant networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[34] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.

[35] E. Hernandez-Orallo, M. Serrat Olmos, J.-C. Cano, C. Calafate, and P. Manzoni, “CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes,” *IEEE Transactions on Mobile Computing*, vol. 14, pp. 1162–1175, June 2015.

[36] E. Davies, G. Tyson, B. Ohlman, S. Eum, A. Molinaro, D. Corujo, K. Pentikousis, and G. Boggia, “Information-centric Networking: Baseline Scenarios,” tech. rep., ICNRG, Internet Draft, RFC 7476, February 2015.

[37] S. Umeda, “Japan: Legal Responses to the Great East Japan Earthquake of 2011,” Sept. 2013.

[38] S. Glenn, “A mathematical theory of evidence,” *Princeton University Press*, 1976.

[39] P. Smets and R. Kennes, “The transferable belief model,” *Artificial Intelligence*, vol. 66, no. 2, pp. 191 – 234, 1994.

[40] T. N. D. Pham and C. K. Yeo, “Detecting colluding blackhole and greyhole attacks in delay tolerant networks,” *IEEE Transactions on Mobile Computing*, vol. 15, pp. 1116–1129, May 2016.

[41] F. C. Lee and C. K. Yeo, “Probabilistic Routing Based on History of Messages in Delay Tolerant Networks,” in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–6, Sept. 2011.

[42] T. Spyropoulos, K. Psounis, and C. Raghavendra, “Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case,” *IEEE/ACM Transactions on Networking*, vol. 16, pp. 77–90, Feb. 2008.

[43] E. T. . 260, “Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC);