This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

A Distributed Trust Management Scheme for Data Forwarding in Satellite DTN Emergency Communications

Philip Asuquo, Haitham Cruickshank, *Member, IEEE,* Chibueze P. Anyigor Ogah, Ao Lei, and Zhili Sun, *Senior Member, IEEE*

***Abstract*—Satellite Communications can be used when other communication systems are either destroyed or overloaded. Observation satellites and Delay/Disruption Tolerant Networks are technologies that can be interconnected to provide emergency communication for disaster recovery operations. DTNs use a store-carry-forward mechanism to forward messages through intermediary nodes to the destination node. The reliability of relaying messages through multi-hop nodes poses a significant problem in DTNs due to lack of consistent connectivity. These network characteristics make DTNs to heavily rely on the cooperation of neighbouring nodes for the successful delivery of packets. However, the presence of malicious or selfish nodes will have a great impact on the network performance. In this paper, we design a decentralised trust management scheme (DTMS) to filter out malicious nodes in DTNs. First, the number of forwarding evidence are combined with the energy consumption rate of the nodes to formulate direct trust. Then, a recommendation trust is computed from the indirect trust, recommendation credibility and recommendation familiarity. Recommendation credibility and familiarity improve the overall recommendation trust by filtering out dishonest recommendations. A comparative analysis of DTMS is performed against a Cooperative Watchdog Scheme (CWS), Recommendation Based Trust Model (RBTM) and Spray & Wait protocol. The results show that DTMS can effectively deal with malicious behaviours in DTNs including trust related attacks.**

***Index Terms*—Delay Tolerant Networks, trust management, routing misbehaviour, emergency.**

Delay/Disruption Tolerant Networks (DTNs) are network architectures developed to cope with intermittent connectivity and long delays 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], [2]. DTNs comprise of nodes with limited resources such as buffer space and power. These constraints in resources, in addition to the sparsity and mobility of these nodes often result in intermittent connectivities. The application of DTN spans across a wide range of domains including Under-Water Networks (UWNs), Pocket Switched Networks (PSNs), Vehicular Ad-hoc Networks, Military applications and Disaster recovery and rescue operations [3], [4]. Recently, there is a growing interest in DTN routing [5]. However, not much attention has been paid to routing misbehaviour. In DTNs, a node can misbehave by dropping packets relayed to it, this can be done intentionally even when the node has sufficient buffer space and contact opportunities. These selfish or malicious behaviours can lead to routing misbehaviours. Although routing misbehaviour has been well studied in MANETs and WSNs, the unique network characteristics of DTNs such as lack of an end-to-end path between nodes, difficulty to predict mobility patterns and long variable delays have made these schemes unsuitable for DTNs [6].

Recent studies on routing misbehaviours in DTNs show that malicious nodes reduce the message delivery probability; nonetheless, a few misbehaviour detection schemes in DTNs [6], [7], [8] have been proposed based on forwarding evidence which are costly in terms of transmission overhead and verification of feedback. These existing approaches proposed in literature do not effectively filter out dishonest recommendations. For example, [9] relies on confidence factor to compute indirect trust. This approach produces a high recommended trust value for indirect trust computation and can result in colluding attacks. Again, evaluating the trustworthiness of a node based on its forwarding behaviour alone may result in an inaccurate trust computation of a node's trust value. Misbehaviour detection schemes such as PMDS [6] will translate to more energy consumption and computational cost which already is a major challenge in DTNs. Popular approaches such as Encounter-Based Routing (EBR) consider encounter value as a metric which is based on pairwise contact probability. EBR is no robust against collaborative attacks. The authors in [10], [11] propose trust management schemes that address selfish behaviours and collaborative attacks in DTNs. However, the proposed solutions do not address routing misbehaviour explicitly. Some of the factors such as connectivity considered in evaluating the trust worthiness of a node are not suitable for DTNs. Other solutions such as COCOWA [12] and CWS [13] focus on the mitigation of selfish behaviour and do not consider other routing misbehaviours.

In this paper, we propose a decentralised trust management scheme which incorporates event familiarity to formulate trust relationship. The trustworthiness of each node is evaluated based on direct and recommended trust relationship formed between nodes. The direct trust is computed based on the forwarding behaviour and the energy consumption rate of the evaluated node. To improve trust computation, we incorporate recommendation trust which is formulated by the combination of recommendation credibility and event familiarity. To

P. Asuquo, H. Cruickshank C. P. A. Ogah, A. Lei and Z. Sun are with the Institute of Communications Systems, University of Surrey, Guildford, GU2 7XH, UK. (e-mail: p.asuquo@surrey.ac.uk; h.cruickshank@surrey.ac.uk; c.anyigorogah@surrey.ac.uk; a.lei@surrey.ac.uk; z.sun@surrey.ac.uk).

Manuscript received July 1, 2017; revised December 15, 2017. (*Corresponding author: Ao Lei*)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

validate our DTMS, we implement extensive simulations in ONE simulator to reflect mission critical scenarios using the Post-Disaster Model (PDM) - RFC 7576 [14] which is a reference model for emergency support and disaster recovery. We compare the performance of DTMS scheme with existing benchmarks schemes when DTN nodes are compromised. Simulation results show that DTMS mitigates individual and colluding packet dropping attackers without incurring high message cost under best trust formation.

The rest of the paper is organised as follows. We review related work in Section II. In Section III, we present the system model and attacks related to trust management schemes. The proposed scheme is presented in Section IV. In Section V, a performance evaluation is carried out and the simulation results discussed. We conclude this paper in Section VI.

I. 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. Every node monitors and evaluates the trustworthiness of its neighbouring nodes. In structured P2P networks, a decentralised trust management scheme which uses a P2P recommender system based on a search tree that is virtually distributed is proposed by [15]. Each peer is assumed to be a trustworthy neighbour unless a complaint is received by the virtually distributed tree search. The authors in [16] propose EigenTrust, 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 [16], a decentralised reputation based trust supporting framework (PeerTrust) with an adaptive trust model for evaluating the trustworthiness of peers based on a transactional feedback system is proposed by [17]. Both EigenTrust and PeerTrust use the trustworthiness of the recommender to evaluate indirect trust. The authors in [18] propose a new fair scheduling technique PowerTrust 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 [19]–[22]. Peers use collective feedback in decision making to mitigate inauthentic file downlands.

There are several trust management schemes proposed for WSNs. One of the first reputation-based frameworks for WSNs (RFSN) was proposed by [23]. RFSN uses two building blocks which include the watchdog and the reputation blocks. The watchdog block is used for monitoring the communication behaviour of the nodes while the reputation block is used to evaluate the trustworthiness of sensor nodes using a Beta distribution framework. In [24], a Parameterized and Localized trUst Scheme (PLUS) is proposed, PLUS uses both direct and recommended trust to build trust relationships among sensor nodes. The integrity of a packet is checked when a trusted node receives a packet from a node that is suspected to be malicious. The trust value of the suspected node is reduced when the integrity check fails irrespective of whether the node was involved in the malicious activity. Another strategy [25] has been proposed for cluster-based WSN. This distributed trust-based framework uses a mechanism to select trustworthy cluster heads. In this approach, trust is modelled using weighing mechanisms of some parameters 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 [26] 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 [27]. 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 [28] 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. Trust Management in Ad-Hoc Networks

In ad-hoc networks, several schemes have been proposed and discussed in a comprehensive survey by [29]. A recommendation based trust model with a defence scheme is proposed to filter trust propagation attacks using clustering techniques [9]. This scheme pays attention to attacks that are related to dishonest recommended from neighbouring nodes at 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 behaviours that are associated with the behaviour of nodes. In the proposed framework, propositions are developed to establish trust through third parties that assist in route selection and malicious node detection. In [31] authors extend the notion of traditional trust to a data-centric 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 a 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

C. Trust Management in DTNs

To maximise delivery ratio and reduce the transmission cost of messages, an Encounter-Based Routing (EBR) [33] 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 evidence. EBR has been widely adopted for DTN routing as most research works in DTNs leverage on its routing strategy. In [10], a novel methodology is proposed to deal with malicious and selfish behaviours. 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, Epidemic and PROPHET routing protocols with a lower message overhead. Similarly, authors in [11] 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 [34] 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 EigenTrust and Bayesian framework [16] under Byzantine attacks. A Probabilistic Misbehaviour Detection Scheme (PMDS) is proposed by [6] based on data forwarding evidence. In this scheme, the inspection game in [35] 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 DTN. 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 [12]. 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 reduction in the detection time and message transmission cost when nodes collaborate using the diffusion module.

D. Summary and research challenges

DTNs are resource constrained networks with limitations in computational, power and communication capabilities which makes them unsuitable for the trust management schemes proposed for P2P, WSNs and Ad Hoc networks. In P2P, the proposed schemes for structured and unstructured overlays cannot be applied to DTNs because the failure of peers will lead to the replication of data across multiple peers thereby exhausting the limited resources in a resource-constrained network. In WSNs, benchmark schemes such as RFSN relies only on direct trust to make forwarding decisions. If the subject node has no previous encounter with the evaluated 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 for routing misbehaviour mainly pay attention to selfish misbehaviour. Game theoretic models such as iTrust effectively detects misbehaving nodes but they are very expensive as a result of the verification cost and the overhead in transmission.

II. Preliminary

In the proposed scheme, trust computation is based on the history of encounters known as the Encounter Record (ER). Suppose two nodes a and b come in contact with each other, ER generated by node a about node b is denoted by $ER_{ab} = (ER_{ab_1}, ER_{ab_2}, ...ER_{ab_n})$ where ER_{ab_i} is a single interaction record with node b.

A. System Model

This paper considers a system model deployed in emergency communication networks [4] as shown in Fig 1. This Post-Disaster Mobility (PDM) model is recommended for Information Centric Network (ICN) baseline scenarios RFC 7476 [14] and similar to the reference scenario described by ETSI [36] for emergency communications. The PDM model imitates the

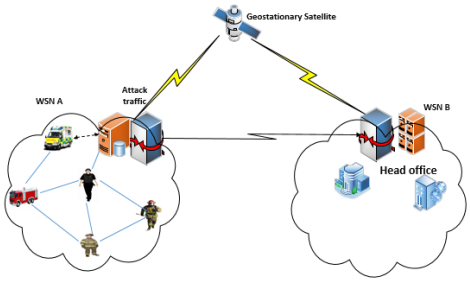


Fig. 1: A Satellite-DTN Emergency Communication Network

situation after the occurrence of a natural disaster. This model assumes that people live in a clustered neighbourhood which is affected by disaster. The post-disaster rescue operation begins after the disaster. Similar to the ETSI Satellite Emergency reference scenario [36], relief centres are set up for the disaster relief and rescue operation. A brief description of the relief centres are described below:

a) Main Coordination Centre: This is the main emergency centre for the coordination of the entire recovery and rescue operation.

b) Relief Camps: Rescue workers are deployed from this centre to the neighbourhood (incident area). Relief materials are also collected from the coordination centre to the relief camps.

c) Evacuation Centre: Each neighbourhood has an evacuation centre, victims in affected areas are evacuated to this centre.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

d) Medical Centre and Hospitals: Medical personnel and paramedics are deployed from this centre to the neighbourhood and evacuation centres

e) Police and Fire Station: Patrol teams and fire trucks are periodically dispatched from this centre to other recovery centres.

The mobility patterns of moving agents captured in the PDM model includes centre-to-centre, convergence-move, cyclic route and event-driven patterns. We pay more attention to the event-driven mobility pattern which is triggered when a specific event is notified to a designated centre as shown in Table 1. Event familiarity can be exploited in the selection of next forwarding node to increase the delivery probability of message to reach the intended recipient.

B. Attack Model

This paper considers individual and colluding attackers. We highlight attacks considered in this scenario that can be performed by malicious nodes in a DTN environment as follows:

a) Dropping Misbehaviour: Just like other participating nodes in the network, malicious nodes receive messages but forward a small percentage of these messages and drop the rest intentionally. Two types of dropping misbehaviours in DTNs are blackhole and greyhole attacks. A blackhole attacker drops all messages relayed to it even if the buffer available is large enough to store the messages. We consider 50% malicious nodes as our worse case scenario.

b) 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 behaviours prevent nodes from relaying packets using the best routes in the networks. Trusted nodes can conspire to propagate these unfavourable rating against healthy nodes.

c) Ballot stuffing attacks: This attack is aimed at misleading the trust management framework to malfunction by providing bad nodes with good reputation based on forwarding evidence. 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 Trust Model

In this section, we present a Decentralised Trust Management Scheme (DTMS) for efficient data forwarding in DTNs. This scheme considers the attacks presented earlier in Section III. The overall trust is computed by direct and recommended trust from the Encounter Record ER generated between two nodes. A statistical model similar to [9] is used to formulate trust relationships. The computation of the trust relationship is based on Beta distribution two class parameter (α, β) used to estimate the probability of expectation. Beta distribution can be computed from Encounter Record ER generated when a node comes in contact with a neighbouring node. The positive and negative interactions are represented as (α, β) respectively. The Beta distribution can be expressed as:

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

where $0 \leq p \leq 1$, $\alpha \geq 0$, $\beta \geq 0$. The two parameters (α, β) can be calculated by accumulations of relayed and dropped messages. In DTNs, delivery probability and the number of dropped messages have been widely used as performance metrics [37], [33], [6], [38]. These metrics have been used in evaluating misbehaviour detection and mitigation schemes proposed for routing, selfish and malicious misbehaviours in DTNs.

A. Direct Encounter Trust

In the model proposed, a direct trust relationship is formed from the ER_{ab} between two nodes a and b at time t. This relationship is expressed as $(\alpha_{ab}, \beta_{ab})$ where α_{ab} and β_{ab} represent positive and negative observations observed by node a about node b. Assuming node a has no contact history with node b, an initial trust value of 0.5 is given to the opinion held by node a about node b. Let s and f represent the positive and negative accumulated evidence from the interactions between nodes a and b. The two class parameter $(\alpha_{ab}, \beta_{ab})$ is computed as

$$\alpha_{ab} = s + 1 \;\; and \;\; \beta_{ab} = f + 1 \tag{2}$$

The direct trust relationship from an ER_{ab} is computed as:

$$T^D_{ab} = \frac{\alpha_{ab}}{\alpha_{ab} + \beta_{ab}} \tag{3}$$

Due to mobility of nodes, the ER table generated changes over time. An adaptive decay λ factor is introduced to decrease the influence of previous observations between nodes a and b before the aggregation of a new trust value. If node a observes an additional event in its ER_{ab} between time t_n and t_{n+1}. The new interactions observed can be expressed as s^{new} and f^{new} for positive and negative behaviours. Before updating $(\alpha_{ab}, \beta_{ab})$, s and f are updated as:

$$s = s^{old} \times \lambda + s^{new} \;\; and \;\; f = f^{old} \times \lambda + f^{new} \tag{4}$$

where $0 \leq \lambda \leq 1$, s^{old} and f^{old} are the old positive and negative interactions observed by node a about the behaviour of node b. When there are no interactions observed between two nodes, s and f are dynamically updated based on the packet forwarding behaviour of the node.

$$s = s^{old} \times \lambda \;\; and \;\; f = f^{old} \times \lambda \tag{5}$$

To obtain the overall direct trust between two nodes a and b, the direct trust T^D_{ab} and the energy trust T^E are computed as:

$$T^{DE}_{ab} = T^D_{ab} W^D_{ab} + T^E_{ab} W^E_{ab} \tag{6}$$

where $W^D_{ab} + W^E_{ab} = 1$, $W^D_{ab} \in [0,1]$, $W^E_{ab} \in [0,1]$ and W^D_{ab} and W^E_{ab} represent the weight values of direct trust and energy trust respectively.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

TABLE I: An Event Table

Event Description	Event	Responder Group 1	Responder Group 2
e_1	Casualty Alert	Relief camps	Moving agents
e_2	Security Alert	Police & Fire station	Ambulance & Fire trucks
e_3	Supplies Alert	Supply vehicles	Ambulance
e_4	EWS Alert	Evacuation Camp	Rescue Workers

Energy Trust: Existing trust management schemes proposed for DTNs do not consider energy trust in formulating of trust relationships between nodes. In resource constrained networks, one of the major challenges is energy consumption. Energy is an important metric in DTNs in view of the fact that messages must be forwarded to active intermediary nodes before it gets to the destination node. In resource exhaustion attacks, malicious nodes can flood messages to neighbouring nodes to deplete the residual energy of encountered nodes. On the contrary, nodes that exhibit selfish behaviours consume less energy due to their non-forwarding behaviour. This scheme considers energy as a QoS metric to ensure that selfish or malicious nodes do not exhaust the limited resources available in DTNs. The evaluation of the forwarding behaviour of a node does not adequately reflect the estimated trust value of a node. A node that has run out of energy can be assumed to be a malicious node. An energy prediction model is incorporated to the direct trust computation to evaluate the reliability of a node in forwarding messages.

The authors in [39] describe the energy model that captures the energy consumption in DTNs. The energy module computes the energy consumption by each node. Several authors [39], [40], [41] have used similar energy modules to compute energy consumption. We use the energy profile described in [39] which has been widely adopted for the analysis of energy consumption in mobile devices. Table 2 presents the energy parameters used to compute the energy consumption. In DTN, a node that has run out of energy can be assumed

TABLE II: Summary of Notations Used

Parameters	Settings
Scan Energy	0.92 mW/s
Transmit Energy	0.08 mW/s
Receive Energy	0.08 mW/s
Initial Energy	4800 Joules

to be malicious since it is not forwarding packet, an energy prediction model is incorporated into DTMS for the evaluation of a node's trustworthiness. The Residual Energy E_R which is the average remaining energy is computed as $E_I - E_C$ where E_I is the initial energy value and E_C is the consumed energy which is computed as $E_C = \{E_s + E_t + E_r\}$ where E_s, E_t, E_r represent the scan, transmit and receive energy respectively. We evaluate the energy consumption of a node as $E_C \in [0, 1]$. The energy trust is computed as:

$$T^E = 1 - E_C \tag{7}$$

T_E must be $\geq$ energy threshold. In the energy module, a punishment factor is introduced which is applied to the weight of T_E if $\frac{E_t}{E_r} < 0.6$. It is assumed that a node exhibits a selfish or a non-forwarding behaviour based if the ratio of E_t and E_r is less than 0.6.

B. Recommendation Trust

One of the characteristics of DTNs is sparse connectivity. Due to lack of end-to-end connectivity, DTNs use a store and carry forward message dissemination approach. A message can be relayed through intermediary nodes till it gets to the destination node. In this situation, a node can get recommendation from neighbouring nodes to evaluate the trustworthiness of an encountered node. To build trust relationships that are reliable, recommendations from encountered neighbouring nodes are incorporated into the trust computation.

Indirect Trust: Assuming nodes a and c have previous contact histories ER_{ac} with each other and node a has no ER with node b but node c has an ER_{cb} with node b. As shown in Fig. 2, node c's direct observation about the behaviour of node b can be used as an indirect trust. The indirect trust of node a about the behaviour of node b observed by node c is computed using $(\alpha^c_{ab}, \beta^c_{ab})$. The indirect trust of node a about the behaviour of node b observed by node c is computed as:

$$R^c_{ab} = \frac{\alpha_{cb}}{\alpha_{cb} + \beta_{cb}} \tag{8}$$

where α_{cb} and β_{cb} are positive and negative events generated from ER_{ac} observed from ER_{cb}. Recommendations from neighbouring nodes often lead to collaborative attacks in trust management systems. To address this, we incorporate recommendation credibility and familiarity values for indirect trust computation.

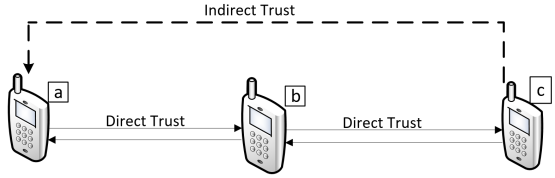


Fig. 2: Direct and Indirect trust

Recommendation Credibility Trust: The main reason for incorporating recommendation trust into the trust management framework is to eliminate false recommendations. A common set of neighbours are considered for trust evaluation. Recommendation credibility is computed from the common neighbours of the evaluating and the evaluated node. As shown in Fig. 3, nodes a and b have common neighbours $c_1, c_2, ..., c_n$. These recommendations are filtered and computed as the recommendations for node b as follows:

$$RC_{ab} = 1 - (T_{c_2 b} - T^R_{b(avg)}) \tag{9}$$

where $T_{c_2 b}$ is the recommendation trust value of node b observed from recommendation c_2 and $T^R_{b(avg)}$ is the average trust value from all recommendations.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

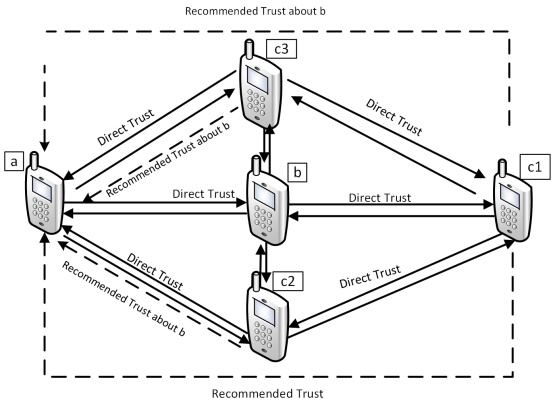


Fig. 3: Computation of recommended trust

Recommendation Familiarity: The concept of familiarity was introduced by the authors in [42] for the web-based product brokering recommendation agents. They point out that trust, confidence and familiarity are different modes of asserting expectation. We adopt the approach similar to [43] to compute this recommendation technique. In recommendation familiarity, the mobility pattern of the responder nodes in the PDM model are taken into consideration. The PDM model is an event-driven model with frequent encounter graphs formed between nodes with frequent inter-contact times from events. Motivated by the concept of social trust in opportunistic networks [44], event similarity is incorporated into the proposed scheme as a recommendation metric to evaluate an encountered node's trustworthiness. This consideration is based on the post-disaster mobility model (Model 1) adopted as a baseline scenario for disaster relief and rescue operations RFC 7476 [14]. The reference scenario for deployment of emergency communication by ETSI for large scale disaster (EQ Scenario) also reflects similar mobility pattern and mobile agents. A brief description of the PDM model is provided in Section III B. Based on the mobility pattern of the responders, we exploit event similarities to enhance the selection of intermediary responders. We use an event feature, $Es = \{e_1, e_2, e_3, ...e_i, ..., e_r\}$ where Es represents the vector of events with r elements as described in Table 1. When an event is triggered, a trust relationship is formulated based on the frequency of similar events or actors. This relationship allows nodes to give more preference to neighbouring nodes with similar event features. The recommendation familiarity is computed as:

$$RF_{ab} = \frac{Es_{c_2b}}{Es_{c_2}} \times \Phi^{\frac{1}{Es_{c_2b}}} \tag{10}$$

where Es_{c_2b} is the number of events in the encounters between nodes c_2 and b based on Es, Es_{c_2} is the total number of events in the encounter record of node c_2 and Φ is the regulatory factor which is used to scale the impacts of the number of encounters, $\Phi \in [0, 1]$. The regulatory factor can be adjusted based on characteristics and environment of the application. The trust value from recommendations is computed based on T^R_{ab}, R^F_{c2b} and $R^C_{c_2b}$. The recommended trust value for the evaluated node b is computed as:

$$T^R_{ab} = \frac{\sum_{i=1}^{n} 0.5 + (T_{c_2b} - 0.5) \times RC_{ab} \times RF_{ab}}{n} \tag{11}$$

C. Overall Trust Value

To obtain the overall direct trust between two nodes a and b, the direct trust T^{DE}_{ab} and the recommendation trust T^R_{ab} are computed as:

$$T_{ab} = T^{DE}_{ab} W^{DE}_{ab} + T^R_{ab} W^R_{ab} \tag{12}$$

where $W^{DE}_{ab} + W^R_{ab} = 1$, $W^{DE}_{ab} \in [0, 1]$, $W^R_{ab} \in [0, 1]$ and W^{DE}_{ab} and W^R_{ab} represent the weight values of direct trust and total recommended trust respectively.

Updating Trust value: Due to the frequent disruptions in DTNs, the computed trust value for each node should be updated periodically. However, when the updates are too frequent, this will result in a high energy consumption. Keeping the trust record window for too long can result in collaborative attacks. A Trust record window is used to update the overall trust value periodically. The trust record window is made up of several time slots for updating trust. Node a evaluates the trustworthiness of node b as $T_{ab}(i) = 1...., t_s$, where t_s represents the number of time slots. The trust value for the next trust record window is updated as

$$T_{ab}(i+1)_{new} = T_{ab(i)} w_{ab(i)} + T_{ab(i+1)} w_{ab(i+1)} \tag{13}$$

where $i = 1, ..., t_s,$, $w_{ab_i} + w_{abi+1} = 1$ and w_{ab_i} and $w_{ab_{i+1}}$ represent the weight values for previous and current trust respectively.

D. Forwarding Decision

The main purpose of the proposed scheme is to ensure that messages are forwarded efficiently to the destination nodes in the emergency communication network. Assuming nodes a and b encounter each other and node a has message for destination node d. Based on the overall trust computation T_{ab}, node a selects node b as its next-hop node based on the following criteria:

1) Nodes a and b come in contact and form an encounter record and event description record.
2) Nodes a and b compute direct trust relationship from forwarding evidence and energy consumption.
3) Nodes a and b compute recommendation trust from indirect trust relationship, recommendation credibility and recommendation familiarity.
4) Nodes a and b formulate a trust relationship based on direct trust and recommendation trust.
5) Nodes a and b exchange their trust record and update their trust tables based on the overall trust value.
6) Node a decides whether to forward a packet through node b based on the trust threshold.

IV. Performance Evaluation

The performance of DTMS is evaluated using Opportunistic Network Environment simulator [45]. ONE simulator is designed specifically for communication in opportunistic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

networks. We simulate the proposed scheme on top of the PDM model. The PDM model was developed by [4] and recommended by IETF [46] for Information Centric Networks: Baseline Scenarios for Emergency Support and Disaster Recovery operations. The Map-Based mobility model constrains the movement of nodes to the paths defined in the map data. The movement models understand arbitrary map data defined in (a subset of) Well-Known Text (WKT). Such data is typically converted from real-world map data or created manually using Geographic Information System (GIS) programs such as OpenJUMP. We use five neighbourhoods, 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 $4,500 \times 3,400$ m , at speeds of $0.5 - 1.5$ km/h for pedestrians and $2.7 - 13.9$ km/h for vehicles. We use 100 pedestrians nodes and 50 vehicular nodes. For each of these scenarios, data traffic is generated as Poisson process at the rate of one message per ten minutes. 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.

The performance of the proposed scheme is compared with RBTM [9], CWS [13] and Spray & Wait (S&W) [47]. RBTM uses Bayesian filtering to probabilistically estimate trust value and incorporates confidence factor, deviation value and closeness centrality value to filter dishonest recommendations. The CWS uses a reputation model which classifies nodes based on their forwarding behaviour and includes a neighbour's evaluation module for indirect trust computation. An efficient and energy preserving scheme (S&W) is also used for comparison. S&W sprays a number of copies into the network unlike flooding protocols like Epidemic. However, it must wait till one of these nodes meets the intended recipients. These schemes are compared using the following metrics:

a) Delivery Ratio: The delivery ratio is the percentage of messages delivered to the total number of messages created.

b) Latency: Latency is computed as the average period of time that a message needs to travel from the source node to the destination node.

c) Overhead Ratio: The overhead ratio measures the delivery cost which is the ratio of the messages relayed to the number of messages successfully delivered to the destination.

d) Dropped Messages: This is total number of messages discarded by nodes due to the expiration of TTL, malicious behaviour or buffer overflow.

e) Detection Accuracy: The percentage of malicious nodes that can be detected correctly.

A. Impact of message dropping misbehaviour on various mobility patterns in the PDM

This subsection compares the impact of the proposed schemes to the other schemes discussed. We address packet dropping attack based on the percentage of misbehaving nodes. We consider $0 - 50\%$ of the nodes in the emergency communication network are malicious. In Fig. 4 (a) delivery ratio, (b) overhead ratio and (c) latency, we explore the performance of DTMS under different traffic patterns in the PDM model. 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, Rescuers-to-Centre (R-C) messages sent by rescuers to centres, Patrol (Police Patrol) and Centre-to-Centre (C-C) which is movement between centres. As observed in Fig. $4(a)$, the delivery ratio decreases as the number of compromised nodes increase. Due to regular patrols, the patrol team have more inter-contact times which reflect on the delivery ratio. The R-C and R-R mobility patterns have lower delivery ratios due to sparse and less meeting times even though they still return to relief centre DTMS reduces the impact of malicious nodes in the network even when 50% of the nodes are malicious. In Fig. 4 (b) and (c), the overhead ratio and latency 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 are reduced.

B. Comparison of message dropping misbehaviour with different approaches

1) Delivery Ratio: In Fig. $5(a)$, the delivery ratio of DTMS, Spray & Wait, CWS and RBTM decreases as the percentage of malicious nodes increase. This is as a result of the number of messages dropped by the malicious nodes. The delivery ratio of Spray & Wait and RBTM decrease rapidly more than DTMS and CWS. Spray & Wait has no mechanism to detect misbehaving nodes while RBTM computes direct and indirect trust using Beta distribution and confidence factor which is proposed for MANETs. As the percentage of malicious nodes increase in the network, RBTM degrades faster than CWS and DTMS. Compared with CWS, DTMS has a higher delivery ratio even with 50% of malicious nodes. In DTMS, the recommendation trust detects more malicious nodes and using the recommendation credibility which aggregates indirect recommendations. The recommendation familiarity enhances the encounter probability to the destination node by choosing nodes with similar event features. In RBTM and CWS, only the forwarding evidence are used to detect malicious nodes. Other features such as energy consumption rate and event familiarity features are not considered. DTMS takes these features into consideration and works better in mitigating malicious behaviour.

2) Overhead Ratio: In Fig. $5(b)$. the results show that RBTM and CWS have a higher over head ratio than DTMS. The clustering procedure applied in RBTMS aggregates recommendations but also leads to a higher routing cost because of the time spent on the computation of the confidence value, deviation value and closeness centrality value. Both CWS and RBTM schemes do not address trust update explicitly. As noticed, the overhead ratio drops as the percentage of malicious nodes increases. This is because the messages are dropped when relayed to the malicious nodes. The overhead ratio computes only the number of messages that reach the destination node. Similar results are observed in [10].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

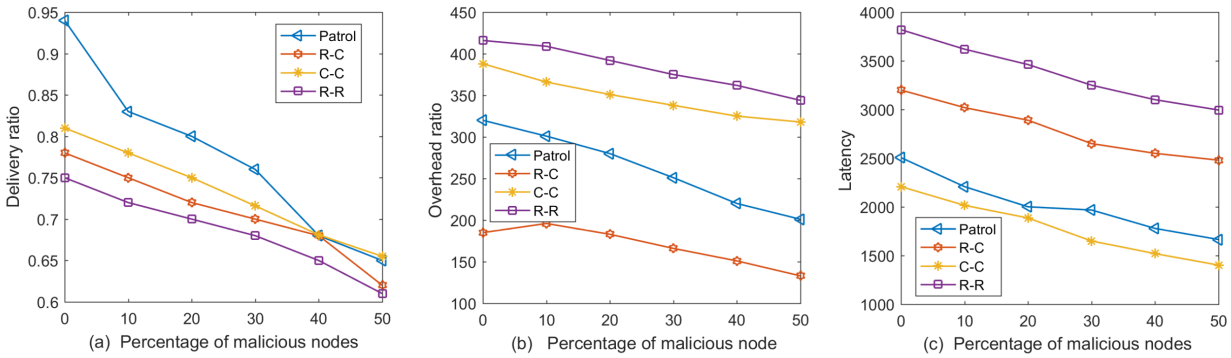


Fig. 4: Performance of DTMS under different mobility patterns in the PDM (Patrol, Rescuer-to-Centre, Centre-to-Centre and Rescuer-to-Rescuer)

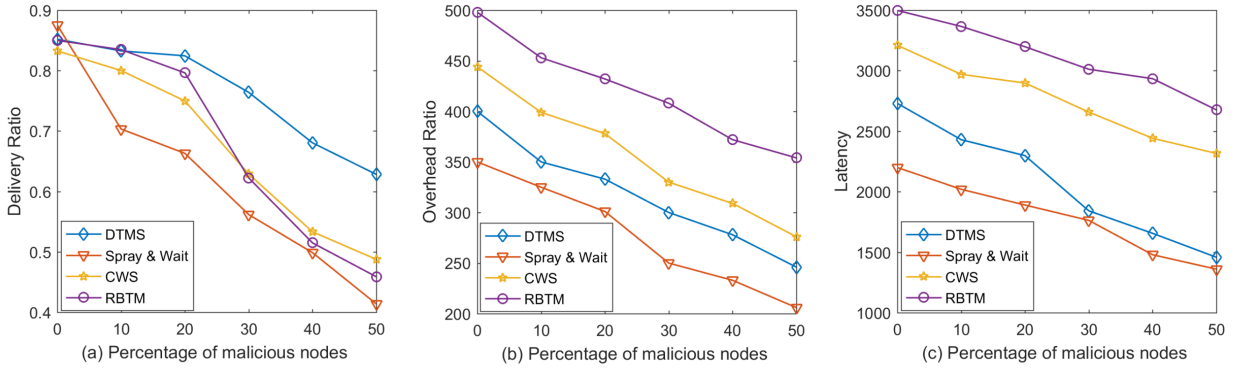


Fig. 5: Performance comparison with other approaches

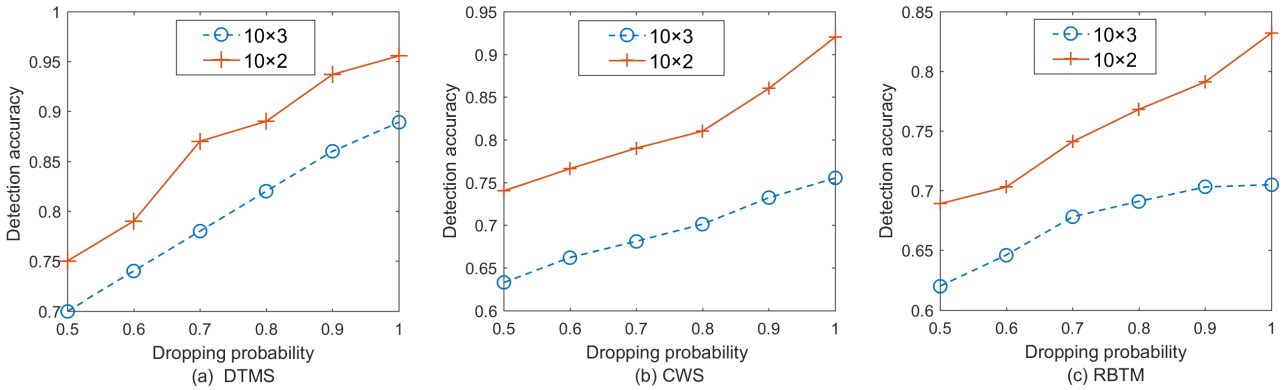


Fig. 6: Detection accuracy of DTMS, CWS and RBTM under varying attack settings

3) Latency: In Fig. $5(c)$, the latency which is the message delivery delay is compared. The main cause of latency in DTNs is retransmission and message queuing. In mobility-aware scenarios, there is a higher inter-contact probability when compared to random waypoint movement model. As expected, the message delay decreases in all approaches. As the number of malicious nodes increase in the network, it takes a longer time to deliver messages to the destination nodes. However, messages with long delays are more likely to de dropped and these dropped messages are not considered when computing the message delay. DTMS performs better than CWS and RBTM when considering the message latency. The results indicate that DTMS reduces the message delay which reflects how quickly it detects routing misbehaviour as the percentage of malicious nodes increase.

4) Detection Accuracy under Collusive Packet Dropping: In this section, the detection accuracy of DTMS is evaluated when nodes collude to drop messages. Malicious nodes collude to drop packets by forming small groups. For clarity, we consider 2 groups of malicious nodes. The first group consists of 20 colluding nodes, represented by 10×2 i.e. two groups of malicious nodes with 10 colluding nodes in each group. The second group has 30 attackers, represented by 10×3 for three groups of colluding nodes. A dropping probability of $0.5 - 1$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2804098, IEEE Journal on Selected Areas in Communications

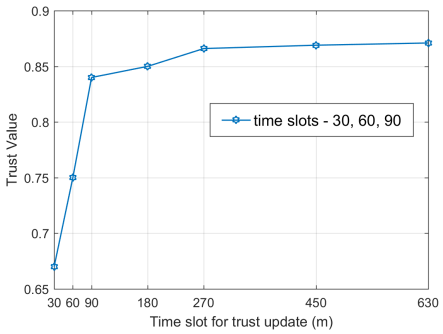


Fig. 7: Trust update with different time slots

is considered. The detection accuracy of DTMS is compared with CWS and RBTM, Spray & Wait is not considered in this evaluation as it does not support malicious node detection. In Fig. 6 (a), (b) and (c), the detection accuracy of DTMS, CWS and RBTM are presented. Compared to RBTM and CWS, DTMS performs better in detecting colluding nodes. DTMS achieves more than 70% accuracy in both colluding scenarios considered. However, the more the number of nodes that collude to drop packets, the lower the detection accuracy.

C. Updating trust value

The percentage of malicious nodes affects the quantified trust value hence the trust value must be dynamically updated. Frequently updating the trust value of nodes will lead to rapid consumption of energy. Again, if the interval for updating the trust value is too long, the current behaviour of the evaluated node is not reflected efficiently. In Fig. 7, we analyse the impact 30% of misbehaving nodes at 30, 60 and 90 mins. It can be observed that after 120 $mins$, the time slots for 60 and 120 mins are almost the same. Therefore, a longer time slot can be used to reduce energy consumption in this case. However, when the percentage of malicious nodes vary, the time slot for each trust update should be reduced especially in mobility-aware or mission critical scenarios.

V. CONCLUSION

In DTNs, trust models have become important in mitigating routing behaviour from compromised nodes. The most common routing misbehaviour in DTN is message dropping which degrades the network performance. Therefore, an adequate and efficient detection mechanism is required to mitigate this routing misbehaviour. In this paper, a decentralised trust management scheme has been designed and validated for mobility-aware DTNs. The proposed scheme combines the forwarding behaviour of nodes and their energy consumption rate to compute direct trust. Second-hand information from neighbouring nodes are also incorporated into the trust model as recommendation trust. The recommendation trust incorporates indirect trust, recommendation credibility and familiarity which is an event based trust. Extensive simulation results show that DTMS effectively mitigates routing misbehaviour such as packet dropping attacks and colluding attacks. In our future work, we will exploit solutions such as using DTN gateways to reduce energy consumption during the computation of direct and recommendation trust.

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, Z. Sun, N. Wang, H. Cruickshank, and N. Ahmad, "A reliable and efficient geographic routing scheme for delay/disruption tolerant networks," *IEEE Wireless Communications Letters*, vol. 2, pp. 603–606, December 2013.

[3] 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.

[4] 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.

[5] Y. Cao, Z. Sun, N. Wang, M. Riaz, H. Cruickshank, and X. Liu, "Geographic-based spray-and-relay (gsar): An efficient routing scheme for dtns," *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 1548–1564, April 2015.

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

[10] 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.

[11] 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.

[12] 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.

[13] J. Dias, J. Rodrigues, C. Mavromoustakis, and F. Xia, "A Cooperative Watchdog System to Detect Misbehavior Nodes in Vehicular Delay-Tolerant Networks," *IEEE Transactions on Industrial Electronics*, vol. PP, no. 99, pp. 1–1, 2015.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

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

[22] 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.

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

[24] 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.

[25] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based 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.

[26] 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.

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

[28] 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.

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

[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 data-centric 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 34,, p. Pages 199214, May-June 2009 2009.

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

[34] 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.

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

[36] E. T. . 260, "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Emergency Communication Cell over Satellite (ECCS)," Technical Specification ETSI TR 103 166, ETSI, F-06921 Sophia Antipolis Cedex - FRANCE, May May 2015.

[37] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 4628–4639, Oct. 2009.

[38] 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.

[39] D. Rodrigues-Silva, A. Costa, and J. Macedo, "Energy impact analysis on dtn routing protocols," *ExtremeCom 12, March 10-14, 2012, Zrich, Switzerland. Copyright 2012 ACM 978-1-4503-1264-6/12/03*, 2012.

[40] T. Abdelkader, K. Naik, A. Nayak, N. Goel, and V. Srivastava, "Sgbr: A routing protocol for delay tolerant networks using social grouping," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 2472–2481, Dec 2013.

[41] M. Uddin, H. Ahmadi, T. Abdelzaher, and R. Kravets, "Intercontact Routing for Energy Constrained Disaster Response Networks," *IEEE Transactions on Mobile Computing*, vol. 12, pp. 1986–1998, Oct. 2013.

[42] S. Y. X. Komiak and I. Benbasat, "The effects of personalization and familiarity on trust and adoption of recommendation agents," *MIS Quarterly*, vol. 30, no. 4, pp. 941–960, 2006.

[43] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for manet based on ahp and fuzzy logic rules," in *2011 IEEE/ACM International Conference on Green Computing and Communications*, pp. 124–130, Aug 2011.

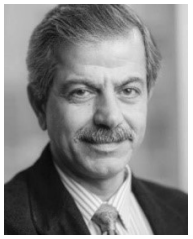
[44] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 594–605, Jan 2016.

[45] A. Kernen, J. Ott, and T. Krkkinen, "The ONE Simulator for DTN Protocol Evaluation," in *Proceedings of the 2Nd International Conference on Simulation Tools and Techniques*, Simutools '09, (ICST, Brussels, Belgium, Belgium), pp. 55:1–55:10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[46] 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.

[47] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking*, WDTN '05, (New York, NY, USA), pp. 252–259, ACM, 2005.

Philip Asuquo received his B.ENG degree in Computer Engineering from University of Uyo, Nigeria and MSc in Computer Network Technology from Northumbria University, Newcastle, UK. He is a PhD candidate in Electronic Engineering at the University of Surrey, UK. His research interest includes Delay Tolerant Networks, Intelligent Transport Systems (ITS) and Wireless Sensor Networks. He is currently a Research Assistant with PETRAS-IoT cyber security hub.



Haitham Cruickshank received a BSc degree in electrical engineering from the University of Baghdad, Iraq, in 1980, and MSc in telecommunications from the University of Surrey, UK and a PhD in control systems from Cranfield Institute of Technology, UK, in 1995. He is a senior lecturer at the Institute of Communication Systems, University of Surrey. His research interests are network security and privacy, satellite network architectures. He has been involved with several European research projects in the ACTS, ESPRIT, TENTELECOM, and IST programmes. He is a member of the Satellite and Space Communications Committee of the IEEE Communications Society, and is also a Chartered Electrical Engineer and IEE corporate.

Chibueze Ogah received the BSc in computer science from the Ebonyi State University, Nigeria in 2005. He received the MSc degree (Distinction) in computer network technology from the University of Northumbria at Newcastle, UK in 2011. He is a PhD candidate at the Institute for Communication Systems, University of Surrey, UK. His research interests include security and privacy in vehicular networks, and Cisco routing protocols.

Ao Lei received his B.Eng degree in communication engineering at Harbin Institute of Technology, China and University of Birmingham, UK, in 2013, MSc degree in communication engineering at the University of York, UK, in 2014, and a PhD in Electronic Engineering from the University of Surrey, UK, in 2017. He is a Research Fellow at the Institute of Communication Systems since 2017.

Zhili Sun received his BSc in mathematics from Nanjing University, China and PhD from the Department of Computing, Lancaster University, UK, in 1991. He is a professor at the Institute of Communication Systems, University of Surrey, UK. His research interests include wireless and sensor networks, satellite communications, mobile operating systems, traffic engineering, Internet protocols and architecture, quality of service, multicast, and security. He has been principal investigator and technical coordinator in a number of projects within the European Framework Program including the ESPRIT BISANTE , TENtelecom VIPTEN, GEOCAST, ICEBERGS, SATELIFE and EuroNGI.