Securing Opportunistic Networks: An Encounter-based Trust-driven Barter Mechanism

Arun Kumar[1]*, Sanjay K. Dhurandher[2], Isaac Woungang[3], and Joel J. P. C. Rodrigues[4,5]
[1]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal,India
arun.k@manipal.edu
[2]Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India
dhurandher@gmail.com
[3]Department of Computer Science, Ryerson University, Toronto, Ontario, Canada
iwoungan@ryerson.ca
[4]Federal University of Piauí (UFPI), Teresina - PI, Brazil
[5]Instituto de Telecomunicações, Portuga
joeljr@ieee.org

Received: December 2, 2020; Accepted: February 10, 2021; Published: June 30, 2021

Abstract

In an opportunistic network (OppNet), message forwarding among the nodes occurs by exploiting the direct contacts through intermittent end-to-end connectivity while relying on the cooperation among these nodes. As such, any misbehavior intention of some nodes may cause serious security threats in the network. To address this issue, several trust-based incentive schemes have been investigated in the literature, with the goal of stimulating the participation of nodes in the routing procedure. However, most of these protocols are susceptible to collusion attacks. In this sense, this paper proposes a secure and reciprocity Encounter-based Trust-driven Barter protocol (denoted ETB), which uses a cryptography mechanism to ensure resilience against collusion attacks in the network. Simulation results show a performance improvement of 19% on average over the IronMan protocol, chosen as benchmark scheme, on account of throughput, average delay, average number of hops, and overhead count.

Keywords: Opportunistic network (OppNet), Opportunistic mobile social network (MSN), Incentive scheme, Trust-driven barter protocol, Reciprocity.

1 Introduction

An opportunistic mobile social network (MSN) is a subclass of OppNets that uses the human social characteristics of nodes to accomplish the message routing and data sharing. As such, it follows the protocol stack model inherited from OppNets [3], where the bundle layer - which sits between the application and transport layers - supports the store-carry-and-forward mechanism. Store-carry and forward scheme is used to enable the routing process in a situation of intermittent end-to-end connectivity and dynamic topology with high delay. In addition, the well-known opportunistic data forwarding strategy used in delay tolerant networks (DTNs)[17] is also applied at this layer for message propagation purposes in the network.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 12(2):99-113, June 2021
DOI:*10.22667/JOWUA.2021.06.30.099*

*Corresponding author: FC-2 Room No 18, Department of Computer Science and Engineering,Manipal Institute of Technology, MAHE, Karnataka, 576104, India, Tel:+91-7037226913

Using the above-mentioned features, numerous routing schemes for OppNets have been designed in the literature[7] under the premise that the node's willingness to participate in the network forwarding is guarantee. However, the nodes in an OppNet are rationally organised through humans, who are often disinclined in sharing their private resources for open causes[20]. Therefore, the above-mentioned routing schemes for OppNets become less attractive in case where the nodes exhibit selfish behavior. As alternatives, credit-based, reputation-based and reciprocity-based incentive protocols for OppNets have been considered in the literature[22]. However, maximum of these schemes are susceptible to collusion attacks. In particular, in cases where colluding nodes launch a bad-mouthing attack[22, 6, 2].

In[1], few reputation-based incentive schemes which address the malicious outsider node attacks using centralized authentication mechanisms have been discussed. In these schemes, the social-centrality based parameters are utilized in the calculation of the trust values of nodes based on non-cryptographic parameter ridden exchange messages. Following the same trend, in this paper, we propose an Encounter-based Trust-driven Barter protocol (ETB). In contrast to the i-Trust scheme[2] which uses a centralized trust authority to identify the malicious nodes, ETB uses a distributed mechanism for the same. Also, unlike the routing scheme proposed in[10], which uses only the previous encounter times when selecting the best next forwarder of a node, ETB uses the encounter vector, along with the message list and exchange list, to construct the so-called history vector used for estimating the final trust value of a node for a given message. The calculated trust value is then used to determine the qualification of node for the forwarding process in the routing.

More precisely, in our proposed ETB scheme, each node maintains an encounter vector, a message list, and a trust vector. Whenever a node, say n_1, encounters another node, say n_2, their encounter vectors are exchanged, and based on an analysis of these vectors, node n_2 generates a claimed certificate against each message in the message list. To avoid non-repudiation, these certificates and encounter vectors are digitally signed. The received claim certificates are intended to prepare the corresponding node (here n_1) to decide on whether to propagate the message to node n_2 or not. At the same time, node n_1 analyzes the encounter vector of node n_2 to determine its former set of encountered nodes, then it verifies the trust vector of those nodes. This trust verification is evaluated by analyzing the certificates and encounter vectors of those encountered nodes.

There are many contributions, cited as follows. First, a trust-based incentive mechanism is designed to support the forwarding process through a barter mechanism for supporting the nodes' cooperation. Second, the proposed scheme provides a solution to the collusion attack by utilizing the RSA cryptographic algorithm[13] to also prevent bad-mouthing attack. To prevent the collaborative nodes to maliciously alter the trust value of any node, the proposed protocol uses cryptography as a means to generate the digital signature for ensuring authentication and non-repudiation. Third, trust-based algorithms are often vulnerable to trust values overestimation, which may lead to uncharacteristic behavior of nodes due to delays incurred in the forwarding process. To avoid this and to ensure resilience in the network, the proposed scheme uses a distributed mechanism to detect overrated nodes and subsequently drop their trust values below a prescribed threshold.

The organisation of remainder section is as follows. In Section 2, related work on incentive mechanisms for OppNet are discussed. In Section 3, the proposed ETB incentive mechanism for OppNets is described. Finally, Section 4 and 5 deliberate on simulation results and conclusion respectively.

2 RELATED WORK

Several incentive schemes for OppNets have been explored in the literature. Li and Das[10] proposed a reputation-based forwarding order for OppNets which uses a positive feedback message (PFM) and the previous encounter times (as features) to select the next best forwarders of a message. Wei et al.[18]

societal awareness quotation-based incentive protocol called SUCCESS. This scheme offers an appropriate way of measuring the metrics of social relationships aimed at community repute and involves the maintenance, updation, and exhibition of the node's reputation tickets based on the requirement. Basha and Mozhi [2] proposed i-Trust, a probabilistic misbehavior recognition scheme for DTNs, in which a intermittently available trusted authority is invoked to judge on the participation of a node to the routing method based on its behavior, which itself is based on collected routing pieces of evidence. Zhu et al.[21] proposed a game theory-based incentive mechanism called i-Trust, which uses the inspection based game on a sequences of newly presented data forwarding evidence. Li et al. [9] designed a reputation-based incentive protocol for data dissemination in mobile participating sensing networks, which promotes the participation of nodes in data delivery based on the calculation of their so-called reputation degrees. The reputation degree of a node is tightly related to its reliability in disseminating the data on accounts of high delivery ratio and low transmission cost.

Jiang et al.[5] designed a credit-based congestion-aware incentive protocol for DTNs, which can effectively upsurge the participation of selfish nodes in message forwarding while following a prescribed delivery delay. A punishment scheme is also implemented to prevent congested nodes from dumping the message in its way to destination. In doing this, the message forwarding procedure is simulated as a bargaining process in which a node is refrained from obtaining more profits by one-sidedly proposing a trading scheme. Xie and Zhang[19] proposed an incentive scheme for DTNs, in which a service priority is used as incentive metric to encourage selfish nodes to cooperate in the message forwarding. To ensure protection against injection and clearance refusal attacks, three low overhead security solutions are proposed, namely cooperation incidence statistics, signature chain and combination consent.

Seregina et al. [14] offered an incentive system for DTNs, in which the selfishness of nodes are calculated by a Central Money Management Center. Using these values, a currency-based trading model is utilized to differentiate the pricing of the node's services, based on which it is decided whether a node is qualified or not to participate in the message forwarding procedure to destination. Himanshu and Madria [4] proposed a reputation and credit-based incentive data-centric dissemination for DTNs, in which the source node annotates the messages with keywords before transmitting them to selected intermediate nodes. These nodes in turn have the option to also add keyword-based annotations to strengthen the message content toward its destination. In doing so, the message security is ensured by means of a distributed reputation model that takes into consideration some parameters such as message quality, relevance of message 'annotations, level of interests, and battery usage. In [16], authors designed a colloborative tracking for managing power in IoT and authors in [15] proposed an efficient and secure protocol for handover in 5G.

Mantas et al.[11] reported on the lack of hard cryptographic-based incentive schemes for OppNets that incorporate both robustness against inaccurate information and resilience towards collusion attacks. Most of these works consider abnormal nodes as selfish, where selfishness is treated as the act of avoiding a voluntary participation in the message forwarding. This is in contrast to real scenarios where selfish nodes are treated as malicious in their actions, i.e. they act to damage the routing and forwarding operations. Qin et al. [12] offered a routing protocol for OppNets, which uses a Markov-based probabilistic prediction model to stimulate cooperation among egocentric nodes. Using of this model, those egocentric nodes with higher probabilities of encountering the destination node are selected by the message carrier as relay nodes to carry the message to its destination. Bigwood et al. [1] designed an incentive mechanism (called IronMan), it uses some pre-existing social evidence to detect and reprimand egocentric nodes that do not cooperate in message forwarding. The IronMan protocol uses a self-reported social network to record the socio-network data for bootstrapping purposes. It exploits the implicit trust relationships to detect selfish behavior and respond to nodes with such behavior by reducing the transmission through them. Because this protocol works on the principle of community-based barter schemes throughout a distributive network setting, its underlying design principles are quite similar to that of our proposed ETB protocol. Therefore, this protocol is used here as benchmark scheme for comparison purpose.

This paper makes use of the notations as depicted in Table 1. In Table 2, a qualitative assessment of few reputation-based incentive schemes against the proposed protocol ETB in terms of monitoring mechanism, observation, reputation propagation, robustness, and resilience against malicious behavior in the network, is provided.

Acronym	Explanation	Acronym	Explanation
EV	Encounter Vector	AHT	Average Holding Time
TE	Time of Encounter	AFR	Average Forwarding Rate
Pr	Private key	SAV	Self-Assessment Value
Pu	Public key	EL	Exchange list
ML	Message list	CCAD	Computing Capacity
CC	Claim certificate	BS	Buffer Size
TV	Trust vector	TAV	Threshold-Assessment Value
HV	History vector	Sec	Security
TA	Trusted Authority	HV	History Vector
PFM	Positive Feedback Mechanism	RV	Reputation Vector
BH	Black-Hole Attack	BM	Bad Mouthing Attack
GH	Grey-Hole Attack	ETB	Encounter-based Trust-driven Barter

Table 1: Acronyms

Paper	Monitoring Mechanism	Direct/Indirect Observations	Reputation Propogation Through	Resilence against Inaccuracy	Punishnment	Robustness against Collusion	Robustness against attacks
i-Trust[2]	TA	Indirect	TA	Yes	No	No	BH,GH
IronMan[1]	HV	Both	Node's Encounters	No	Yes	No	No
Radon[10]	PFM	Both	Node's Encounters	No	No	No	BH
Success[18]	RV	Both	Nodes in the same community	No	Yes	No	BH
ETB	HV/RT	Both	Node's Encounters	Yes	Yes	Yes	BH,BM

Table 2: Comparision of ETB against few reputation based incentive schemes

3 ETB DESIGN

3.1 Design Assumptions

In our proposed ETB schemer, a barter mechanism is designed based on the Tit-for-Tat concept, which involves the introduction of random egotistical behavior of nodes in the network. The selfish-reluctant nodes have a random probability p of participation with an encountered node. The design considers the case of collaborative bad-mouthing attack and the RSA algorithm [13] is used to ensure the authenticity and integrity of the messages in the network. Each node in the system is assumed to possess at least the public keys of its x associated neighbors for ensuring hop-to-hop authentication. The proposed design includes the consideration of dense OppNet topologies with high-end computing nodes in order to support edge computing. Also, in this design, the adversaries are considered as internal to the network, and they collaborate in the miscalculation of the trust using the bad-mouthing attack.

3.2 Data Structures

The proposed ETB mechanism maintains and uses the following data structures for its functional requirements:

3.2.1 Encounter vector

A node i retains an encounter vector EVi that holds the evidence of the encountered nodes j along with their time of encounter TEi(j). It also holds the encrypted TEi(j) (using the private key of node j) to prevent the network from non-repudiation. This data structure is shown in Figure 1.

Enc_Node	$TE_i(j)$	$Pr_j(TE_i(j)$

Figure 1. Encounter Vector

3.2.2 Message List

In OppNet, the intermediate nodes use the concept of storecarryandforward to carry the message on the way to its destination. In doing so, the message list ML_i of a node i comprises the messages along with their attributes for forwarding the same. Each message M in ML_i at node i is attributed a unique message sequence number (MS_No). The message M is also associated with characteristics such as size, source ID (S_Id), destination ID (D_Id), previous hops with encountered time (PH), $TE_i(j)$, and desired quality of service (QoS). The QoS comprises of the desired throughput DT_i, delay (DD_i), number of hops (DH_i) and message security requirement in the network as shown in Figure 2.

MS_No	*S_Id*	*D_Id*	*Size*	*PH,*TE_i	DT_i	DD_i	DH_i

Figure 2. Message Vector

3.2.3 Exchange List

This refers to the exchange message list $EL_i(j)$ at node i for node j. The encounter node i resolves the forwarding of message M in ML_i on the merit of the encountered node j's claim certificate $CC_ji(M)$. In $EL_i(j)$, node i holds the Msg_Seq_No of the exchange message M along with the received claim certificate $CC_ji(M)$ as shown in Figure 3.

Msg_Seq_No	$CC_j(M)$

Figure 3. Exchange List

3.2.4 Trust Vector $TV^i_{t_k}[N]$

This vector is used to maintain and hold the trust for all the encountered nodes in the network at time t_k.

3.2.5 History Vector HV_i

The ML_i and $EL_i(j)$ lists at node i are processed regularly to capture the average holding time AHT_i and forwarding rate AFR_i of messages in the network. In doing so, the history vector HV_i holds the dynamic value of AHT_i and AFR_i that will be further used in the calculation of the self-assessment value $SAV_ji(M)$ for the claim certificate $CC_ji(M)$ from node j corresponding to message M in the list ML_i.

3.3 Proposed ETB Scheme and Algorithm

As stated earlier, any node i in the network maintains the data structures ML_i, EV_i, $EL_i(j)$, $TV^{i}_{t_k}[N]$, and HV_i,. The frequent update of these vectors on the node' encounters and message forwarding necessitates the design of a trust configuration strategy in the proposed incentive mechanism. Indeed, let's assume that a node i encounters a node j at time t_k. Both nodes i and node j register their encounters in their respective encounter vectors EV_i and EV_j with the privately encrypted timestamp t_k for thwarting the non-repudiation attack. The encryption of the encounter time t_k using the private key of the encountered node also helps in protecting against the bad-mouthing attack. The Encounter vector is also used as a piece of evidence to challenge the non-repudiation and the bad-mouthing attack using the encrypted claim certificate. After registration of the encounters of nodes i and j in their respective encounter vectors, both nodes share their corresponding message lists. Now, suppose that a node i shares its message list ML_i with node j. Node j then uses the trustvector TV_j and history vector HV_j to assess the probability of forwarding with the desired QoS in terms of self-assessment value $SAV_ji(M)$ for each message M in ML_i.

Further, after receiving the claim certificate $CC_ji(M)$ for message M in ML_i, node i decides on inducting the message M in the exchange vector $EL_i(j)$. Next, the self-assessment value $SAV_ji(M)$ is compared against a prescribed threshold value calculated based on the desired QoS parameters. Afterwards, if the $SAV_ji(M)$ for message M is higher than the desired threshold value, then the message M is inducted in the exchange list $EL_i(j)$. Once this threshold calculation is completed for all the messages in the message list ML_i along with the formation of the exchange lists $EL_i(j)$, the transfer of messages in the exchange list $EL_i(j)$ occurs from node i to node j. The message list ML_i at node i is then further updated after the exchange of $EL_i(j)$ to node j and the receipt of $EL_j(i)$ from node j. During this process, the RSA algorithm [10] is used to secure the hop-to-hop communication between nodes i and j through ensuring the authenticity and integrity of the message.

Now, let's assume that a node j meets node k at time t'_k,where t'_k is greater than the time t_k of the previous encounter of node j with node i. Then, as usual, the exchange of the encounter vectors, message lists, and exchange list will take place between nodes j and k. The exchange of these vectors also ensures the updating of their corresponding data structures. Now let's suppose that at time $t''_k(t''_k > t'_k > t_k)$, node k meets node i. After receiving EV_k, node i comes to know about the encounters of node k with node j at time t'_k. Further, a node i claims to node k about the encounters of node j at time t'_k. In response to this claim, node k requests the node i for the digitally signed encounter vector as evidence. After verification of the received evidence, node k requests node i to share the vector $EL_i(j)$. Next, node k processes $EL_i(j)$ along with ML_j, $EL_j(k)$, and $CC_kj(M)$ to ascertain whether node j has computed $EL_j(k)$ as per the claim certificate $CC_kj(M)$. Afterward, if node k notices any kind of deviation from the standard processing, then it will depreciate the trust value of node j in the trust vector $TV_k[N]$ and will share the collected evidence with subsequent encountered nodes in the network.

In our proposed scheme, trust depreciation is a way to punish (resp. incentivize) the node for cooperation and participation in the network. In this mechanism, the trust depreciation information is propagated to the encountered nodes in the network. Thus, non-collaborative nodes may collude and disseminate the false trust depreciation information in the form of a bad-mouthing attack, which it is worth noting that it has been thwarted using a secure mechanism of hop-to-hop authentication and integrity. Here, at the time of sharing the trust depreciation information, a node is asked to provide privately encrypted pieces of evidence in terms of the claim certificate of an encounter vector. The verification of this evidence helps in curbing bad-mouthing attacks in the network. Besides, nodes in the trust-based algorithm may collude to increase the trust of any malicious node in the network. The malign trust increment of an adversary node may misrepresent the adversary as a highly trusted central node in the network. The high centrality of a malicious node provides an added advantage to a node to introduce an undesirable delay in the message transmission and packets drop at will, which may lead to a blackhole attack. In our proposed scheme, to balance the overestimation of the trust, each node processes an encounter vector of the encountered node over a period of time. The repeated calculation of trust helps in determining those nodes whose centrality values are more significant than the average centrality value in the network. Then, the over-estimated central node' trust values are re-adjusted and configured to counter the possibility of black hole/wormhole attack. Therefore, an unnecessary delay in the message forwarding process is avoided. It should be noted that our proposed ETB scheme uses the claim certificates in terms of self-assessment value (SAV) for each message in the message list. The calculation of the self-assessment value $SAV_ji(M)$ at node j for message M considering node i depends on the following factors: number of adjacent neighbor nodes Adj_j; HV_j; buffer size BS_j; computing capacity $CCAD_j$ at node j; security feature $Seq_j(i)$ at node j for node i; number of current flow requests $N\_Flow\_Req_j$ at node j; and traffic type $TT_j(i)$. It should be noted that $SAV_ji(M)$ is directly proportional to the neighbors' forwarding rate FR_j, buffer size computing capacity, and security options. On the other hand, the average holding time and the number of previous hops indirectly impact the calculation of $SAV_ji(M)$. Hence, we get the following equations

$$SAV_ji(M) \propto (Adj_j, FR_j, BS_j, CCAD_j, Seq_j(i)) \tag{1}$$

$$SAV_ji(M) \propto \frac{1}{(TT_j, AHT_j, No\_Prev\_Hops)} \tag{2}$$

$$SAV_ji(M) = K\frac{F_1(Adj_j, FR_j, BS_j, CCAD_j, Seq_j(i))}{F_2(TT_j, AHT_j, No\_Prev\_Hops)} \tag{3}$$

Where for practical purpose, the functions F_1 and F_2 can be considered as linear and additive and K is a self-assessment constant value (set to 1 in our calculation). The claim certificates of a node j for message M considering node i is the public encryption of the privately encrypted $SAV_ji(M)$. Hence, $CC_ji(M) = Pu_i(Pr_j(SAV_ji(M), t_k))$ is the claim certificate from node j for node i considering message M. The selection of message M in the exchange list depends on the comparison of TAV with SAV. Node i calculate the threshold assessment value (TAV) for message M in ML_i as follows:

$$TAV_ij(M) = F_3(Desired\_throughput, Desired\_delay, Desired\_hops, Desired\_security) \tag{4}$$

Where the function F3 is also considered as linear and additive. If $SAV_ji(M)$ is larger than or equal to $TAV_ij(M)$, the message M is encompassed in the exchange list $EL_i(j)$. The pseudo-code of the planned ETB algorithm is given in an algorithm 1. The algorithm's complexity is in the order of O(m), where m represents the amount of messages at a time in the message list of the node. This algorithm has implemented at the network layer, where the intrinsic forwarding mechanism has also been adjusted.

Algorithm 1: ETB Algorithm on encounter of node i with j

```
while (1) do
    if Encounter of node i with j then
        1: Exchange Encounter Vector ($EV_i$; $EV_j$) and Message List ($ML_i$; $ML_j$).
        2: Nodes i and j calculate Threshold assessment vector $TAV_ij(M)$ and $TAV_ji(M)$ respectively.
        3: Nodes i and j calculate self-assessment vector $SAV_ji(M)$ and $SAV_ij(M)$ respectively.
        4: Encrypt $SAV_ji(M)$ and $SAV_ij(M)$ to get claim certificates $CC_ji(M)$=$Pu_i(Pr_j(SAV_ji(M),t_k))$ and$CC_ij(M) = Pu_j(Pr_i(SAV_ij(M),t_k))$
        5: if $TAV_ji(M) > SAV_ij(M)$ include M in $EL_j$ and if $TAV_ij(M) > SAV_ji(M)$ then include M in $EL_i$.
        6: Exchange Exchange List $EL_j$and $EL_i$.
        7: Nodes i and j probe EVi and EVj to ascertain whether they have encountered nodes k and k' respectively.
        8: Nodes i and j check the $EL_k$ and $EL'_k$ along with $CC_ki(M)$ and $CC_kj(M)$ respectively.
        9: Upon verification of $CC_ki(M)$ and $CC_kj(M)$, node i and j calculate the trust depreciation and register these values in $TV_i$ and $TV_j$ respectively.
        10: Node i (resp. j) upon encountering any other node $k''$ share the trust depreciation along with the required encrypted evidences.
        11: Nodes i and j probe encountered vector respectively to determine whether the central node has a centrality value greater than the threshold value.
    else
        do nothing;
    end
end
```

4 PERFORMANCE EVALUATION

In this section, the performance of the designed ETB incentive scheme is gauged using the ONE simulator [8], then compared against that of the IronMan scheme [1] on account of throughput, average end-to-end delay, an average number of hops per message, overhead count, and the number of false positives, chosen as performance metrics, under varying buffer size, TTL, percentage of selfishness in the node, and proportion of selfish nodes in the network. Here, it should be mentioned that the overhead count refers to the number of forwarded counts, which also includes the cost connected with message forwarding. On the other hand, the number of false positives is compared against the varying percentage of nodes' selfishness and the percentage of selfish nodes in the network.

4.1 Simulation Setup

The trace file of nodes' contact obtained from the Haggle project, is utilized for simulation purposes. The trace file takes account of 78 short radio ranges imotes and 20 stationary long-range radio imotes. The scanning granularity of a Bluetooth enabled nodes are set at once per 120 seconds along with pairwise contact frequency of 6878 per day. An average duration of contact is 216 seconds with total number of contacts took place is 23,478. The ONE simulator[8] is used to re-produce the events based on the log accounts of the INFOCOM 2006 data-trace file. The selfish behavior has been introduced in all the nodes with a randomly varying selfish level. Each time after an observed contact, the concerning nodes exchange and update their respective data structures (mentioned in section 3.2) for evaluating the claim certificates through proper consideration of requirements concerning message exchange.

4.2 Simulation Results

First, the TTL for the message is constant and set to 2880 minutes. It is assumed that 20% of nodes are selfish, with the introduction of 50% selfishness in them. The buffer size is varied from 40 MB to 140 MB, and the impact of this variation on the throughput, delay, number of hops, and overhead count, is examined. The results are presented in Figure. 5 - Figure. 8.

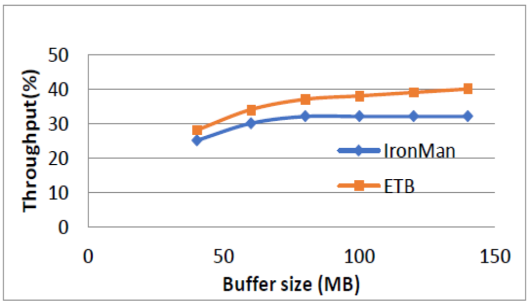

Figure 5: Throughput vs. Buffer size.

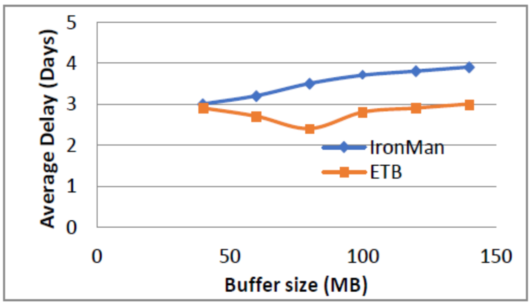

Figure 6: Average delay vs. Buffer size

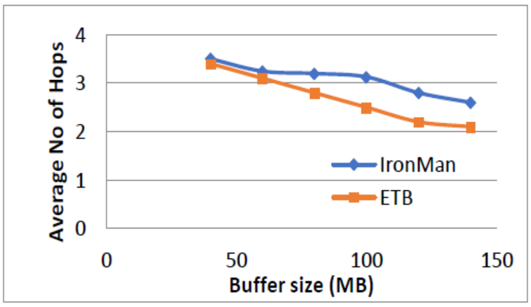

Figure 7: Average number of hops vs. Buffer size.

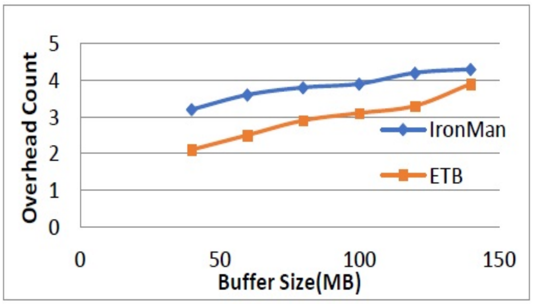

Figure 8: Overhead count vs. Buffer size.

In Figure. 5, it is witnessed that an increase in buffer size yields an upsurge in the throughput for both Iron Man and ETB. On average, the throughput of ETB is 20% more than that of the IronMan protocol. This gap is more pronounced when the buffer size is equal to 140 MB. Meantime, ETB requires buffer spaces for maintaining the vectors used for determining the self-assessment value. In Fog. 6, it is observed that initially, in the case of ETB, there is a decrease in the delay by a significant margin of 720 minutes, which is attributed to its intrinsic incentive strategy. It can also be perceived that ETB outclasses IronMan in terms of the average delay incurred during message delivery. Figure. 7 shows that with the increase in buffer size, the ETB reduces the average number of hops from 3.4 to 2.1. In Figure. 8, it is found that the overhead count for ETB is less than that of IronMan. This can be attributed to the fact that ETB uses the concept of self-assessment value in terms of claim certificate, and the messages are exchanged only with the authentic and probable high trust nodes in the network.

Second, it is presumed that 20% of nodes are selfish, with the introduction of 50% selfishness in them. The buffer size fixed at 100 MB and the TTL is varied. The bearing of this variation on the throughput, delay, average number of hops, and overhead count, are examined. The results are shown in Figure. 9 - Figure. 12 In Figure. 9, it is detected that when the TTL increases, the throughput initially increases from 29% to 38%, then starts decreasing subsequently. Indeed, initially, the buffer size of 100 MB supports the increase observed in the throughput. Then, an increment of TTL beyond 2880 minutes exhausts the limited sized buffer, thereby reduces the throughput considerably from 38% to 30%. In Figure. 10, it is witnessed that initially, the limited buffer of size 100 MB has helped in reducing the delay by a margin

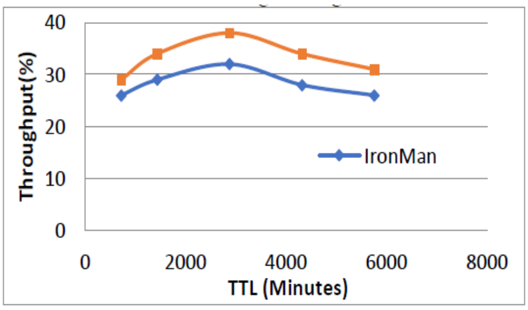

Figure 9: Throughput vs. TTL.

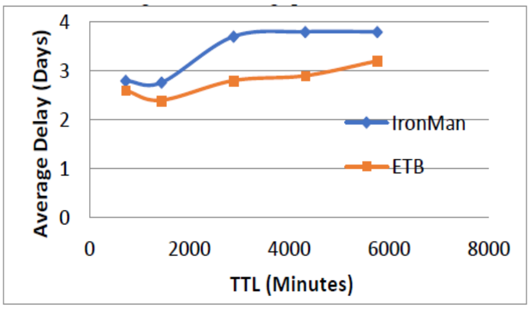

Figure 10: Average delay vs. TTL.

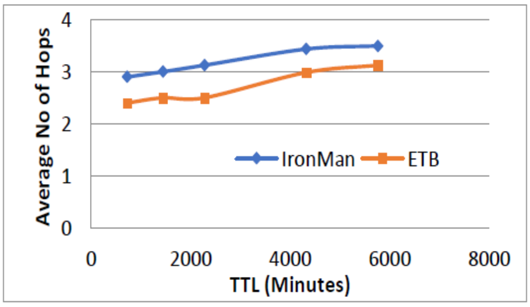

Figure 11: Average number of hops vs. TTL.

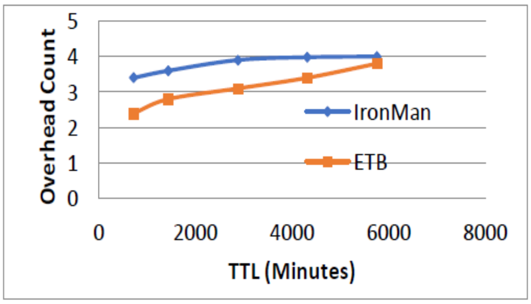

Figure 12: Overhead count vs. TTL.

of around 512 minutes. Further, with the increase in TTL, the delay has also increased, but the growth is less pronounced for ETB compared to IronMan. In Figure. 11, it is found that when the TTL is augmented, the average number of hops also increases, but ETB yields less number of hops compared to IronMan. The steep rise of 0.5 hops with the increase of TTL from 2880 minutes to 4320 minutes is mainly credited to the low involvement of nodes in the forwarding procedure and the exhaustion of the assigned 100 MB buffer space. In Figure. 12, it is perceived that ETB yields less overhead ratio equated to that generated by IronMan.

Third, the selfishness level of the nodes is adjusted, and the influence of this variation on the throughput, delay, average number of hops, and overhead count, is evaluated. The results are given in Figure. 13 - Figure. 16. In Figure. 13, it is pragmatic that ETB maintains its throughput at 40% whereas the throughput of IronMan is continuously fallen as the selfishness level increases from 0% to 40%. A drop of 10% is observed for the ETB protocol when the selfishness level is in the range [40%, 60%]. However, when the selfishness level for all nodes is 100%, the throughput of ETB and IronMan are below 5%. In Figure. 14, it is witnessed that the increase in delay for ETB is considerably lower than that of IronMan under the selfishness level range of [0%-40%]. Beyond that level, the exhaustion of buffer is responsible for the observed increase in delay for ETB compared to IronMan.

Figure. 15 represents the situation where the ETB maintains an average number of hops close to 2 under varying selfishness range from 0% to 20% and buffer size fixed at 100 MB. Consequently, the overhead count is increased steeply and is well in tune with that of IronMan for a selfishness level of nodes higher than 20% (as depicted in Figure. 16). Figure. 17 characterizes the behavior of throughput against the varying level of selfishness in the network. It is observed that ETB maintains an average 36% of throughput compared to a continuous decrease of the same in the case of IronMan protocol. Fourth, the selfishness level of nodes is kept static at 50% and the number of selfish nodes in the network is varied. The bearing of this variation on the delay, average number of hops, and overhead count, are explored. The results are represented in Figure. 18 - Figure. 20.

In Figure. 18-20, it can also be detected that when the percentage of selfish nodes is in the range [0%-40%], ETB yields less delay, hop counts, and overhead count compared to IronMan. Fifth, the

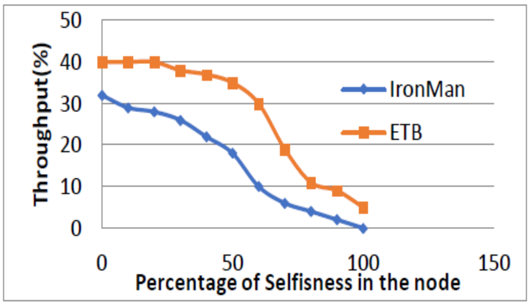

Figure 13: Throughput vs. Selfishness level in node.

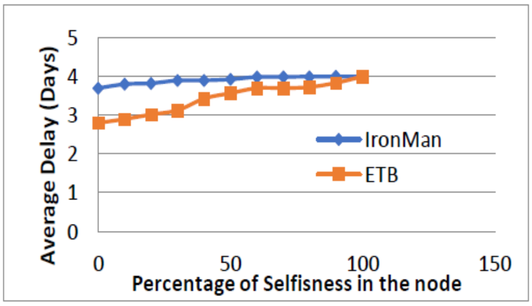

Figure 14: Average delay vs. Selfishness level in node.

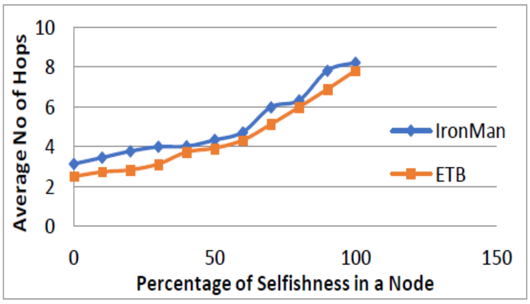

Figure 15: Average number of hops vs. Selfishness level in node.

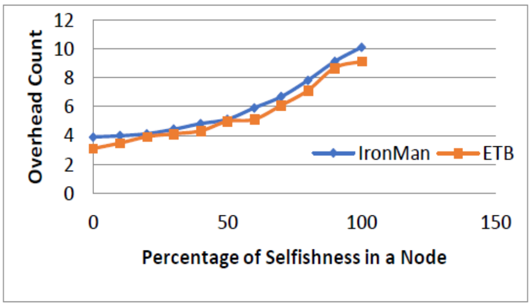

Figure 16: Overhead count vs. Selfishness level in node.

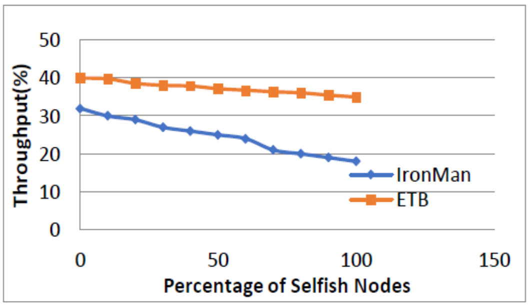

Figure 17: Throughput vs. Number of selfish nodes.

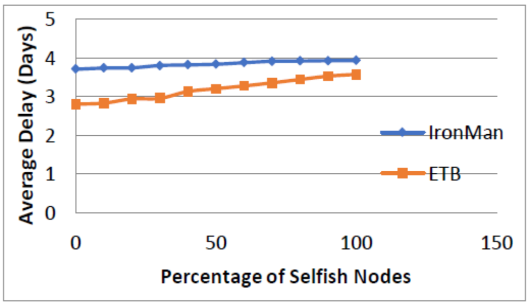

Figure 18: Average delay vs. Number of selfish nodes

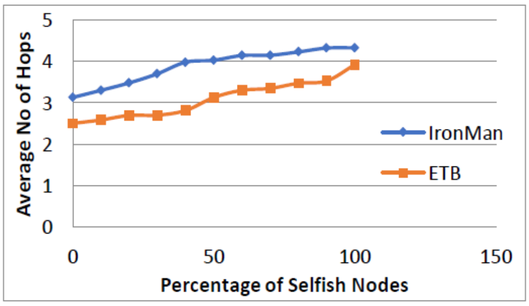

Figure 19: Average number of hops vs. Number of selfish nodes.

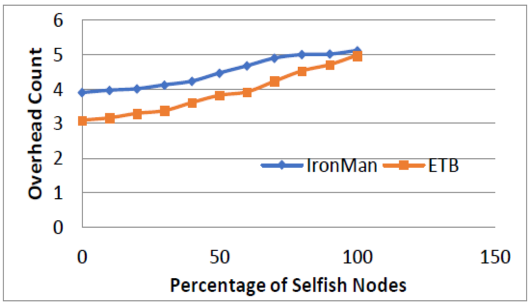

Figure 20: Overhead count vs. Number of Selfish Nodes.

percentage of selfish nodes is varied, and the bearing of this variation on the rate of false positives is evaluated. The results are represented in Figure. 21. It can be witnessed that when the selfishness level of nodes is in the range [0%-40%], the average percentage of false positives is less than 7%. On the other hand, once the selfishness level of nodes goes above 50%, the rate of false-positive increases sharply. However, when selfishness level is 50%, the rate of false-positive is below 10%, even when there are 100% selfish nodes in the network.

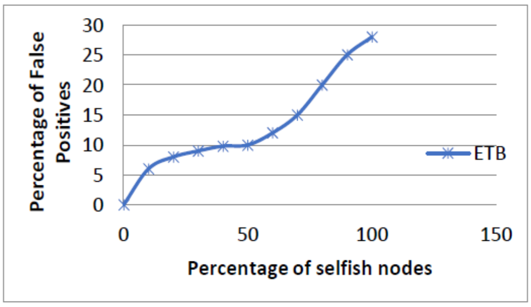

Figure 21: False Positive Rate vs. Selfishness Level in Node.

The proposed design is based on assumption of nodes with high end computing facility in dense OppNet settings. So, the designed schem is not suitable for sparse remote topological settings and the use of RSA for ensuring security aslo makes it unsuitable for limited comuping nodes. Designed scheme is ensuring security only against colloborative bad-mouting attack. Hence, there is still possibility of improving the design to cater to the demand of defending against other colloborative attacks in the network. In the proposed scheme energy consumption is more and thus scheme can be accentuated to work in limited resource environment, on account of both power and computation. In comparision to other related incentive schemes based on barter mechanism, proposed scheme defends against the colloborative bad-mouthing attack using evidence based scheme facilitated through RSA. The designed incentive mechanism is conceptulised to support the forwarding process along with evidence based incentive scheme.

5 CONCLUSION

This paper has proposed a TFT-based secure incentive scheme (called ETB) for OppNets, in which a verification process is implemented by means of exchanging digitally signed claim certificates using a public-private key-based cryptography mechanism. The proposed ETB scheme is also designed to protect against bad-mouthing attack. Simulation results have shown a better performance of the ETB scheme (about 19% improvement) compared to the IronMan scheme in terms of throughput, delay, the average number of hops, and overhead count. As future work, we plan to make ETB energy-efficient and compare its performance against that of few energy-efficient benchmark routing mechanisms for OppNets.

Acknowledgments

This work is partially supported by a grant from the National Science and Engineering Research Council of Canada (NSERC), Reference: RGPIN-2017-04423, held by the 3rd author, and a grant from the National funding from the FCT – Fundação para a Ciência e a Tecnologia through the UID EEA/500008/2013 Project, and by Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017-5, held by the 4th author.

References

[1] G. Bigwood and T. Henderson. Ironman: Using social networks to add incentives and reputation to opportunistic networks. In *Proc. of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (SocialCom'11), Boston, Massachusetts, USA*, pages 65–72. IEEE, October 2011.

[2] J. Du, G. Han, C. Lin, and M. Martinez-Garcia. Itrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*, Early Access:1–1, October 2020.

[3] C. Huang, K. Lan, and C. Tsai. A survey of opportunistic networks. In *Proc. of the 22nd International Conference on Advanced Information Networking and Applications - Workshops (WAINA'08), Gino-wan, Japan*, pages 1672–1677. IEEE, March 2008.

[4] H. Jethawa and S. Madria. Reputation and credit based incentive mechanism for data-centric message delivery in dtns. In *Proc. of the 2018 19th IEEE international conference on mobile data management (MDM'18), Aalborg, Denmark*, pages 207–216. IEEE, June 2018.

[5] Q. Jiang, C. Men, and Z. Tian. A credit-based congestion-aware incentive scheme for dtns. *Information*, 7(4):71:1–21, December 2016.

[6] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293 – 315, September 2003.

[7] N. Kayastha, D. Niyato, P. Wang, and E. Hossain. Applications, architectures, and protocol design issues for mobile social networks: A survey. *Proceedings of the IEEE*, 99(12):2130–2158, November 2011.

[8] A. Keränen, J. Ott, and T. Kärkkäinen. The one simulator for dtn protocol evaluation. In *Proc. of the 2nd international conference on simulation tools and techniques (Simutools'09), Rome, Italy*, pages 1–10. ICST, March 2009.

[9] J. Li, X. Wang, R. Yu, and R. Liu. Reputation-based incentives for data dissemination in mobile participatory sensing networks. *International Journal of Distributed Sensor Networks*, 11(12):172130, December 2015.

[10] N. Li and S. K. Das. Radon: Reputation-assisted data forwarding in opportunistic networks. In *Proc. of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp'10), Pisa, Italy*, page 8–14. ACM, February 2010.

[11] N. Mantas, M. Louta, E. Karapistoli, G. T. Karetsos, S. Kraounakis, and M. S. Obaidat. Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: a survey. *IET Networks*, 6(6):169–178, November 2017.

[12] X. Qin, X. Wang, L. Wang, Y. Lin, and X. Wang. An efficient probabilistic routing scheme based on game theory in opportunistic networks. *Computer Networks*, 149:144–153, February 2019.

[13] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[14] T. Seregina, O. Brun, R. El-Azouzi, and B. J. Prabhu. On the design of a reward-based incentive mechanism for delay tolerant networks. *IEEE Transactions on Mobile Computing*, 16(2):453–465, February 2017.

[15] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38 – 57, January 2018.

[16] F. Song, M. Zhu, Y. Zhou, I. You, and H. Zhang. Smart collaborative tracking for ubiquitous power iot in edge-cloud interplay domain. *IEEE Internet of Things Journal*, 7(7):6046–6055, July 2020.

[17] K. Wei, X. Liang, and K. Xu. A survey of social-aware routing protocols in delay tolerant networks: Applications, taxonomy and design-related issues. *IEEE Communications Surveys & Tutorials*, 16(1):556–578, May 2014.

[18] L. Wei, H. Zhu, Z. Cao, and X. S. Shen. Success: A secure user-centric and social-aware reputation based incentive scheme for dtns. *Ad Hoc & Sensor Wireless Networks*, 19(1):95–118, January 2013.

[19] Y. Xie and Y. Zhang. A secure, service priority-based incentive scheme for delay tolerant networks. *Security and Communication Networks*, 9(1):5–18, October 2016.

[20] K. Xu, P. Hui, V. O. K. Li, J. Crowcroft, V. Latora, and P. Lio. Impact of altruism on opportunistic communications. In *Proc. of the 2009 First International Conference on Ubiquitous and Future Networks (ICUFN'09),*

Hong Kong, China, pages 153–158. IEEE, July 2009.

[21] 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*, 25(1):22–32, January 2014.

[22] 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*, 58(8):4628–4639, October 2009.

Author Biography

Arun Kumar is an Assistant Professor at Manipal Institute of Technology, Karnataka, India and completed his Ph.D in Opportunistic networks from CAITFS lab in NSIT, Delhi University in the year 2018. He received his M.Tech degree in Computer Science from School of Computer and System Sciences (SC&SS), Jawaharlal Nehru University Delhi in year 2012. He has also worked as Research Officer at Auckland Univeristy of Technology, New Zealand on health science project. His research interest includes Opportunistic Networks, IOT and Vehicular area Networks, Virtual reality and Machine Learning.

Sanjay Kumar Dhurandher received the M. Tech and Ph. D degrees in Computer Science from the Jawaharlal Nehru University, New Delhi, India. He is presently working as a Professor in the Department of Information Technology, Netaji Subhas University of Technology (Formerly NSIT) New Delhi, India. He is also the Head of the Department of Information Technology at NSUT. From 1995 to 2000 he worked as a Scientist/Engineer at the Institute for Plasma Research, Gujarat, India which is under the Department of Atomic Energy, India. He is currently serving as an Associate Editor for the "International Journal of Communication Systems" and "Security and Privacy Journal" published by John Wiley & Sons. His current research interests include wireless adhoc networks, computer networks, network security, underwater sensor networks, opportunistic networks and cognitive radio networks. Presently, he is also a Senior Member of IEEE and Fellow of IETE.

Isaac Woungang received his Ph.D. degree in Mathematics from University of South, Toulon and Var, France, in 1994. From 1999 to 2002, he worked as Senior Software Engineer at Nortel Networks, Ottawa, Canada. Since 2002, he has been with Ryerson University, where he is now a Professor of Computer Science and Director of the DABNEL Research Lab. His current research interests include radio resource management in next generation wireless networks, computer security, computational intelligence and machine learning applications, performance modelling, and optimization. He has published 8 edited books, 1 authored books, and over 80 refereed journals and conference papers.

Joel J. P. C. Rodrigues is a professor at the Federal University of Piauí, Brazil; senior researcher at the Instituto de Telecomunicações, Portugal; and collaborator of the Post-Graduation Program on Teleinformatics Engineering at the Federal University of Ceará (UFC), Brazil. Prof. Rodrigues is the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), an IEEE Distinguished Lecturer, Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis – Covilhã Science and Technology Park. He was Director for Conference Development - IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications co-Chair. He is the editor-in-chief of the International Journal of E-Health and Medical Communications and editorial board member of several high-reputed journals. He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored over 950 papers in refereed international journals and conferences, 3 books, 2 patents, and 1 ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a member of the Internet Society, a senior member ACM, and Fellow of IEEE.