New Trust Based Smart Data Forwarding Mechanism in Vehicular Delay Tolerant Network

[1,2]Seema Jangra and [3]Amit Kant Pandit
[1,3]Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir, India.
[2]Indraprastha College for Women, University of Delhi, New Delhi, Delhi, India.
[1,2]sjangra@ip.du.ac.in

Correspondence should be addressed to Seema Jangra : sjangra@ip.du.ac.in

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202404077
Received 12 March 2024; Revised from 06 June 2024; Accepted 04 July 2024.
Available online 05 October 2024.

Abstract – Vehicular Delay Tolerant Network (VDTN) is the growing field with a considerable possibility to handle future wireless application's requirements. Using vehicles for the data communication purpose can be contemplated as a substitute for the wired and wireless systems. This paper proposes a trust-based data forwarding mechanism for Vehicular Delay Tolerant Network (VDTN). Data forwarding in VDTN requires every vehicular or stationary node to participate in data forwarding. But some time malicious nodes show non-cooperative behaviour in data forwarding. Therefore, malicious nodes must be identified specifically to accelerate the data forwarding. A threshold based social skeleton membership process along with new trust-based data forwarding mechanism is proposed in this paper. We reveal that the social skeleton members perform better in data forwarding in terms of data delivery ratio, data delay and data overhead. Simulation results demonstrate that the trust-based data forwarding improves the data delivery ratio with trust-based data forwarding approach. After simulation a comparative analysis of two different scenarios is presented with epidemic routing, prophet routing and spray and wait routing.

Keywords – Opportunistic Networks, Social Skeleton, Threshold, Trust Based, Vehicular Delay Tolerant Network.

I. INTRODUCTION

Vehicular Delay tolerant Network (VDTN) is a kind of Delay Tolerant Network (DTN) [1] with mobile nodes. VDTNs have intermittent connectivity among vehicular nodes and road side units (RSU) to forward messages by employing store-carry-forward paradigm [2, 3]. Different routing protocols like epidemic, MaxProp, Prophet and DFEMD [2] are also used in forwarding the message. Data transmission in Vehicular Delay Tolerant can be possible when all the mobile nodes may cooperate with each other in transmission with VDTN's characteristics like high delay, variable data rate and network partitioning. Due to the presence of these characteristics and the absence of reliable centralized authority, VDTN is vulnerable to different types of threats and attacks. The bundles (message) are passed between different communicating nodes using store-carry and forward approach [4]. The propagation of bundles buffered at intermediate nodes depends on type of the contact i.e., opportunistic contact or scheduled contact.

In opportunistic contact or scheduled contact, the communication links established are insecure and unreliable due to the dynamic topology. For reliable and secure communication in VDTN, the activity or behaviour of vehicular nodes should be monitored. VDTN has the same kind of vulnerabilities, threats and attacks as exist in another wireless network except for the absence of an end-to-end connectivity [5].

The various security goals in a vehicular environment are availability, authentication, confidentiality, integrity, privacy, and non-repudiation [6]. VDTNs are fundamentally decentralized and entirely rely on node's cooperation and their participation in bundle forwarding [7].

To ensure secure and trusted communication, socially dissimilar nodes should be identified and data should be routed through the trusted nodes. In the present paper, a reliable data forwarding approach is proposed. The proposed approach used a social skeleton of trusted vehicular nodes which contribute in the data forwarding with more efficiency. The paper is structured in different sections: related background work is presented in section 2, social skeleton and social skeleton membership process depicted in section 3 and section 4 respectively. Proposed data forwarding approach through trust based social skeleton is depicted in section 5. Experimental setup is presented in section 6 followed by section 7 conclusion of the paper.

II. LITERATURE REVIEW

In DTN, nodes send the data packets to its neighbouring nodes with assumption that the adjacent nodes help in data transmission towards the destination node. However, this is not always true and any node in the network can behave unexpectedly. These misbehaving nodes can perform active attacks as well as passive attacks.

Misbehaving node does not participate in the routing process. This kind of node intends to interrupt the function of the network. A misbehaving node can harm the network intentionally or unintentionally. It can drop the received data packets, delayed the data packets, and floods the packets on the available network to interrupt the service or to consume the resources like bandwidth and memory. In the presence of such threats, a reliable interaction among the different nodes is required. Misbehaving nodes are categorized into two categories: malicious node and selfish node [7, 8].

Malicious Node

A node is titled as malicious node if it has an intention to harm the network. These types of nodes can harm the network by performing various attacks. The malicious node can insert many packets in the network to drain the network resources [9, 10]. Malicious node targets to interrupt the routing services by dropping the packets. They can do either selective dropping (Gray hole attack) by selecting the designated packet, from the selected node and at a selected time or can drop every packet (Black hole attack) [11, 12]. Despite this dropping attack, malicious nodes can perform some attacks related to the trust of nodes. Self-prompting attacks, bad-mouthing attacks, and ballot stuffing attacks are an example of such attacks [13].

Selfish Nodes

Sometimes, nodes present in the network drops the data packets or do not forward them intentionally for their personal gain. These types of nodes are called selfish node. Selfish nodes drop the packets due to different reasons, one of them is to save their resources like energy and storage [14]. They do not receive the data packets or if received then do not forward them. Selfish nodes can be individual selfish and social selfish [15]. Sometimes selfish nodes forward the data packets only due to the social ties. These types of nodes are non-cooperative in nature towards the nodes having no social ties. Individual Selfish node drops all the data packets coming from all other nodes in the network.

Despite of these types of nodes some nodes perform packet dropping attack but not intentionally. The reason for packet drop can be scarce resources, Hardware/Software problem or insufficient memory or power to forward the node [16]. These types of nodes are cooperative, but sometimes they misbehave unintentionally.

To control the selfish node, a credit-based mechanism based on the combined trust value of a DTN node is proposed in [1]. The combined trust vale is calculated by an agent. The backtracking approach is also used for left nodes which are not covered by the agent node.

Before the data packets forward to the neighbor node, trustworthiness of the neighboring node should be evaluated for successful transmission of data packet. Trust is the symbol of reliability in social behavior. It helps in evaluating the relationship between more than one object [17]. Trust among the human being can be considered as an assurance that the activities of that human being will lead to positive upshots [18]. In network security, trust was introduced as the main component [19]. In the network, trust can be used in the context of reliability, honesty, and reputation of two entities for a defined task [20]. Different trust management schemes ensure the degree of healthy relationships and cooperation among the different nodes and reputation of an individual node.

Due to node heterogeneity and mobility, it is not possible that all the participated nodes are cooperative with each other and remain trustworthy. Due to the lack of an end-to-end connectivity, successful delivery demands more cooperation among the nodes as compare to MANET or Ad-hoc network. DTNs and VDTNs are very vulnerable to different attacks, particularly inside attacks that decline the network's performance. To detect the presence of misbehaving nodes and their associated attack in DTNs, many trust management techniques are proposed by researchers. Misbehave detection approaches can be a detective and preventive [21].

Detective techniques detect and remove the packet dropping misbehaving nodes by using encounter-based strategy, watchdog, rate limit certificates, incentive-based and Merkle-Hash-Tree [7].

Preventive approaches try to encourage the nodes to cooperate by using incentive schemes, credit-based schemes, reputation-based schemes, and barter based schemes [22]. Preventive schemes prevent the dropping of the packets by the misbehaving node.

The various parameters that can be used to calculate the trust value of a node are no of packets forwarded, no of contacts, duration of contact and similarity index value. Based on the values of these parameters, a node can be classified as malicious node or selfish node [23].

Using different parameters, several detection techniques have been proposed by different researchers. In encounter (contact between two nodes) based detection approach [8] every node records the details of all the information regarding contact like the time of encounter, frequency (number of encounters), encountered node's id and number of packets forwarded with the sequence number. Based on this information, the detections of the misbehaving node can be done. In the detective approaches the watch dog-based scheme is used to detect the selfish node [24]. In this cooperative approach, each node examines the performance of his neighbor node and based on the performance, it assigns a

reputation value and classification unit classify the node according to the reputation value. Cooperative value is calculated based on the classification to punish or reward the node.

Another approach used to detect the misbehaving node is rate-limiting with claim-carry and check approach [25]. Rate limiting is to detect the flood attack and packets claim-carry and check strategy is used to reduce the complexity of counting. Incentive-based detection/prevention schemes are used to deal with misbehaving nodes using different techniques. Reputation-based schemes, barter-based schemes, and credit-based schemes incentive-based approaches. In Reputation-based detection approach, a reputation's threshold value is used to detect the legitimacy of a node. Reputation value higher than the threshold value encourages the neighbor nodes to accept data packets from the node. The reputation value increased whenever the node forwards the data packets and decrease when dropping the data packets. The node having a low reputation does not accept data packets, or an acknowledgment of the receiver can calculate it. Trusted authority (TA) based reputation can be either global or personal.

A credit-based approach SMART is proposed in [24] to deal with selfish nodes in DTN. This secure multilayer credit base scheme is used to stimulate the forwarding process by many incentive techniques. The credit-based approach can be divided further into three categories Message Purse Model-based, Message Trade, and TA-trade-model based. These three schemes depend on the payment of credit. In Message Purse Model-based scheme the source node makes the payment of credit. While in Message Trade Model-based (MTM) destination nodes make the payment of credit. When other than source or destination makes the payment of credit, then the scheme is TA-trade-model based. To mitigate with the selfish node or malicious node, a routing protocol based on social contribution (SCR) is proposed in [25]. Delivery ratio and social influence are the two factors considered while making packet forward decision. Node's delivery ratio depends on the social influence, which can be used to push the misbehaving nodes to contribute in data routing positively.

Another incentive approach is barter based (bargaining based/conditional forwarding) detection approach used to motivate the suspected node to be cooperative. Different algorithms are used in [22] to mitigate misbehave or selfishness.

To defence against faking packet attack, a new detection and trace back mechanism is used based on Merkle-Hash-Tree. In this technique, each authentic node can identify the attack using a Merkle tree hashing approach. The technique is divided into two parts, i.e., attack detection followed by node traceback. In the first part, the attack is identified by the legitimate node by calculating the Merkle root hash value and compare with old value (calculated by source node). Based on the difference between these two values, the authentic node can trace back to find the malicious node. In Markle Hash Tree, the hash value is calculated from the bottom to top using post-order (left, right, and root).

An acknowledgment-based packet dropping attack detection is proposed in [20]. Acknowledgment given by Intermediate node to the source node is used in the Merkle tree, and root value is compared with the old root value to detect the packet dropping. To check and detect packet integrity attack Merkle tree-based detection approach is also proposed in [22].

III. SOCIAL SKELETON

The subset of the heterogeneous social vehicular node's network and road side stationary nodes opportunistically connected with each other to forward the information is considered as social skeleton. The social skeleton is designed to establish the communication between vehicular nodes with trust and reliability. In the social skeleton the subset of vehicular nodes can communicate with each other and forward the data to the subset of node that also belong to the social skeleton. The selection of gateways (Road Side Unit) provides the interface for the communication between the nodes belongs to the different groups i.e., different social skeleton and outside the social skeleton group. The various parameters and characteristics of the social skeleton group are defined by the common road side unit.

IV. SOCIAL SKELETON MEMBERSHIP PROCESS

In VDTN, communication cannot be possible without cooperation between two nodes. In order to achieve efficiency and reliability (security) in communication, node's behaviour should be evaluated. The factors affecting the reliability and trustworthiness of a node can be subjective and objective in nature. The objective properties are dependency, reliability, and punctuality. Subjective properties include honesty, unselfishness, and integrity.

The social skeleton membership of a vehicular node is defined by the common road side unit (RSU) in the vehicular network. The road side unit will categories the vehicular nodes in two groups based on the different parameters. The two groups are defined as social skeleton group and unsociable group. The road side unit define the membership of each group.

Membership Parameters

Social skeleton membership parameters are as follows:

Present Behavior Observation Parameters

In present behaviour observation, a trusted node R investigates the behaviour of the other node to check the trustworthiness or reliability. Observational trust depends on the node's data exchange and data treatment policies. The

behavioural parameters/attributes that influence the trustworthiness of a node are its contact frequency, contact duration, and the number of packets forwarded.

Contact Frequency

Contact Frequency is defined as the number of encounters between the vehicular nodes and RSU. More the number of encounters between V_i (Vehicular node) and V_j (vehicular node or RSU) in duration t, higher is the trust. The contact frequency between V_i and V_j or RSU can be calculated as shown in Eq. (1).

$$CF_{V_i}(t) = \sum_{V_j=0}^{N} CF_{V_i,V_j}(t) \tag{1}$$

Where $CF_{V_i}(t)$ is the total number of contact frequency, $\sum_{V_j=0}^{N} CF_{V_i,V_j}(t)$ is the sum of contact frequency between V_i and its single hop neighbours V_j, j=0…N during time t.

Contact Duration

The contact duration of two vehicular nodes V_i , V_j reflects the trust value. Contact duration is directly proportional to the trust value shown in Eq. (2).

$$CD_{V_i}(t) = \sum_{V_j=0}^{N} CD_{V_i,Vj}(t) \tag{2}$$

Where $CD_{V_i}(t)$ is the total value of contact duration of Vi during time t. $\sum_{V_j=0}^{N} CD_{V_i,Vj}(t)$ specify the sum of contact duration of V_i and all its single hop neighbours during time t where V_j=0……N.

Number of Packets Forwarded

Trust value of a node increase with high packet forward ratio. If a node forwards number of packets, it means the node may not drop the data packets usually. Packet forward ratio is calculated according to Eq. (3).

$$PFR_{V_i}(t) = \frac{PF_{V_i}(t)}{\sum_{V_m=1}^{N} PR_{V_i,V_m}(t)} \tag{3}$$

Where $PFR_{V_i}(t)$ represents the packet forward ratio of V_i and $PF_{V_i}(t)$ is the number of packets forwarded by V_i . $\sum_{V_m=1}^{N} PR_{V_i,V_m}(t)$ is the total number of packets received by V_i from its single hop neighbours.

Hence, after examining all the parameters, trust value based on the present behaviour observation is calculated by using weighted summation of all three parameters. $T_{V_i,R}^{Obs}$ is calculated by using Eq. (4).

$$T_{V_i,R}^{Obs} = W^{CF} * CF_{V_i}(t) + W^{CD} * CD_{V_i}(t) + W^{PF} * PFR_{V_i}(t) \tag{4}$$

Where W^{CF}, W^{CD}, and W^{PF} represent the weight associated with each behavioural attributes of the trustee node, i.e., contact frequency, contact duration and the number of packets forwarded respectively.

Similarity Parameter

In similarity parameters, RSU examines the common properties between the two vehicular nodes V_i, V_j. The common properties include social properties and physical properties. Vehicular node's social properties include the social relationship with another vehicular node like community and friendship. The nodes belonging to the same community or having common friends shows more similarity towards each other. Transmission range, transmission speed, vehicle's moving speed, mobility pattern, location, time of the visit to RSU are the physical properties that can be considered to evaluate the similarity of trust. Higher similarity index represents more trust. Similarity trust index between V_i and V_j is calculated by using the Jaccard similarity method as shown in Eq. (5).

$$S_{V_i,V_j}^{X} = \frac{S_{V_i}^{X} \bigcap S_{Vj}^{X}}{S_{V_i}^{X} \bigcup S_{Vj}^{X}} \tag{5}$$

Where $S^X_{V_i,V_j}$ is the similarity index of social property between V_i and V_j concerning the social properties X. $S^X_{V_i}$ and $S^X_{V_j}$ represent the set of social properties (X) of V_i and V_j, respectively.

$$P^Y_{V_i,V_j} = \frac{P^Y_{V_i} \bigcap P^Y_{Vj}}{P^Y_{V_i} \bigcup P^Y_{Vj}} \tag{6}$$

In Eq. (6). $P^Y_{V_i,V_j}$ is the similarity index of physical property between V_i and V_j concerning the physical properties Y. $S^Y_{V_i}$ and $S^Y_{V_j}$ represent the set of social properties (Y) of V_i and V_j, respectively.

The similarity trust is calculated by the weighted summation of the social property similarity index $S^X_{V_i,V_j}$ and the physical property similarity index $P^Y_{V_i,V_j}$ see Eq. (7).

$$T^{Simi}_{V_i,V_j} = W^X * S^X_{V_i,V_j} + W^Y * P^Y_{V_i,V_j} \tag{7}$$

Where $T^{Simi}_{V_i,V_j}$ is the similarity trust between V_i and V_j. X and Y represent the social properties and physical properties, respectively. W^X and W^Y are the weight associated with social properties and physical properties.

Membership Eligibility Computation

Trust value parameters of node V_i are evaluated by RSU. The total trust value of a vehicular node is calculated by using Eq. (8).

$$T_{V_i,R}(t) = W^1 * T^{Obs}_{V_i,R} + W^2 * T^{Simi}_{V_i,V_j} \tag{8}$$

Here $T_{V_i,R}(t)$ is the total trust value. W^1, W^2 are the weights associated with each parameter i.e., present behaviour observation and similarity parameters, respectively. $T^{Obs}_{V_i,V_j}$ is behaviour observation trust and $T^{Simi}_{V_i,V_j}$ is similarity trust.

The vehicular node exchanges the value of parameters with RSU by exchanging a summary vector that holds the behavioural parameters value and similarity parameters value. The RSU calculates the node's trust value according to Eq. (8).

While computing the value of total trust, the value of weight associated with each parameter can be considered accordingly.

The membership of the vehicular node for the social skeleton group is decided by the value of total trust $T_{V_i,R}(t)$ as shown in **Table 1**.

Table 1. Membership Eligibility

Node's Trust Value	Group Membership
$T_{V_i,R}(t) < 1$	Unsociable
$T_{V_i,R}(t) \geq 1$	Social Skeleton

If the trust value of the vehicular nodes computed by the RSU is less than 1 (weights are assigned to each parameter accordingly), the RSU nominated the vehicular node for an unsociable group. If the trust value of a vehicular nodes computed by the RSU is greater than 1, the RSU nominates the vehicular node for the social skeleton group.

V. PROPOSED DATA FORWARDING THROUGH TRUST BASED SOCIAL SKELETON

Data forwarding to the neighbour node must ensure that data should reach its destination successfully with minimum time and minimum resource consumption. In this proposed data forwarding approach shown in **Fig 1** data is forwarded by the vehicular node to the neighbour node if it belongs to the same social skeleton group. Let us consider RSU as road side unit and two vehicular nodes $V_iV_iV_iV_i$and V_jV_j encounter with each other. Data forwarding with the proposed approach can take place using the following steps:

1. Initialise the lookup table of Road side unit (RSU) and vehicular node(V).
2. Initialise the summary vectors (SV).
3. Exchange of summary vectors on encounter of vehicular nodes with RSU.
4. Based on the summary vector, RSU computes the trust value of the vehicular node V_i by using weighted summation of all the parameters and updating the lookup table.

5. If the trust value of vehicular node V_i is $T_{v,R}(t) \geq 1$, then RSU nominated the vehicular node for the social skeleton group. If the trust value of vehicular node V_i is $T_{v,R}(t) \leq 1$, then RSU nominated the vehicular node for the unsociable group.
6. The updated lookup table is exchanged against the summary vector to each vehicular node and they update their own table.
7. Vehicular node $V_iV_iV_iV_i$encounters the vehicular node V_jV_j and wants to forward the data; it will look in to the lookup table and if the node V_jV_j belongs to the same social skeleton group V_i V_i forward the data to nodeV_jV_j.

   If the node belongs to the unsociable group data transmission does not take place between two dissimilar group's members.
8. Lookup table in each vehicular node made them communicate with social skeleton group members. The members of an unsociable group require getting authentication from the RSU to forward the data to the vehicular node of the social skeleton.

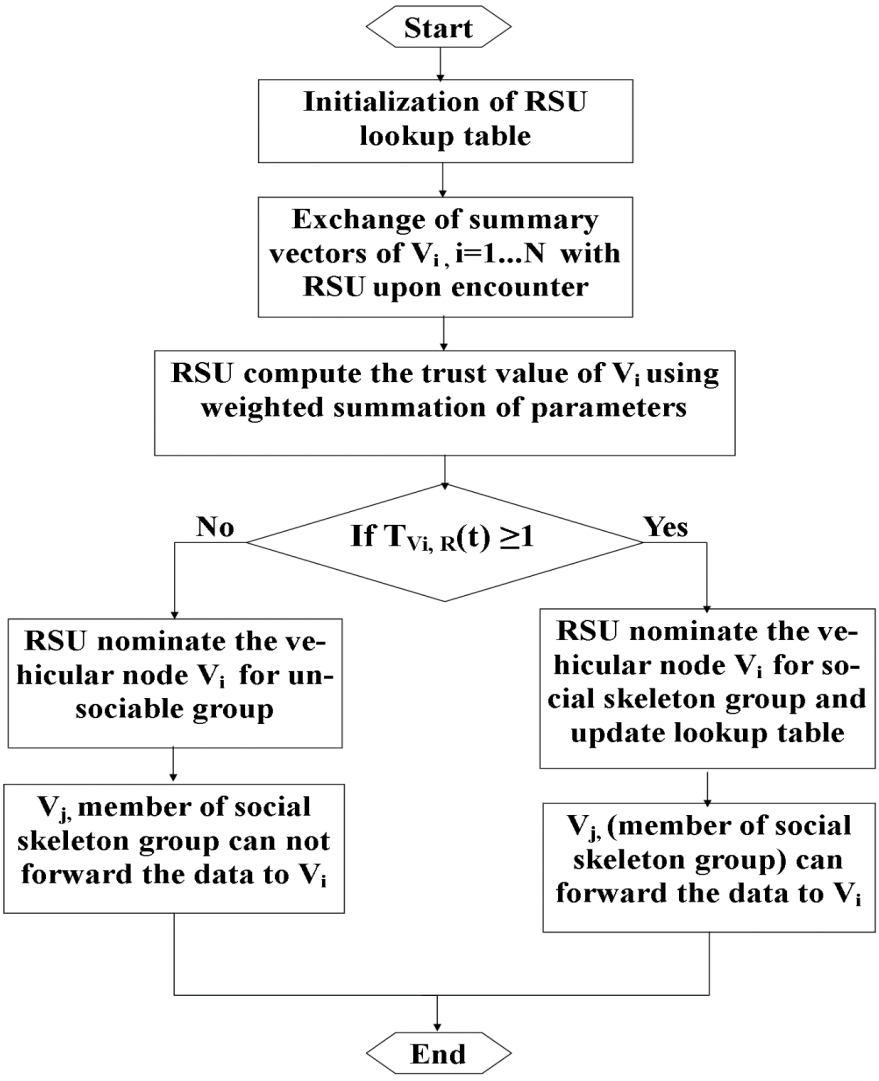

Fig 1. Data Forwarding Process in Trust Based Social Skeleton.

VI. EXPERIMENTAL SETUP

Opportunistic network environment (ONE) [17] is simulation software that is used for Opportunistic Network Environment. This simulation software is specially designed for simulating DTNs involving opportunistic contacts between the nodes. The routing protocol used in DTNs, mobility models and terrain properties can be specified and simulated using this ONE Simulator tool.

Scenario Description

Two scenarios are considered to evaluate the proposed social skeleton: Network model with trust-based routing in Social Skeleton and Network model without trust-based routing in social skeleton but with benchmark routing protocols. Both models are considering the area of Jammu's local towns like Katra, Reasi, Akhnoor, Domel and Shri Mata Vaishno Devi University (SMVDU).

Design of Social Skeleton

Social Skeleton is designed using heterogeneous trusted nodes with different kinds of interfaces like high-speed and Bluetooth. It also contains some road side unit stationary nodes having both interfaces and behaving as a gateway in the network model. The first scenario was designed without a social skeleton using a bluetooth interface for data transfer among the nodes while the second scenario was designed with a trust based social skeleton using bluetooth interfaces. The area is bounded within 100 km square of range with a total of 213 nodes for both scenario settings as shown in **Fig 2**. The road side unit is the trusted or common friend stationary node that provides the recommendation trust.

In the first scenario without a social skeleton, Domel town comprises 10 pedestrians, 4 cars, and 10 stationary nodes. Katra city comprises 20 pedestrians, 16 stationary nodes, and 4 cars. 10 nodes are kept stationary, 10 nodes as pedestrians and 4 nodes are cars located in SMVDU. 4 car nodes, 20 pedestrian nodes and 16 stationary nodes are placed in Reasi and Akhnoor towns. 80 car nodes, 25 pedestrian nodes and 20 stationary nodes are also placed randomly in the whole bounded area. All the nodes present in this first scenario have a bluetooth interface. The Map Route movement model is used for specified routes.

In the second scenario with a social skeleton, Domel town comprises 10 pedestrians, 2 cars and 4 stationary nodes having bluetooth interface only, 4 stationary nodes (RSU) and 2 cars with high-speed communication interface only and 2 cars with bluetooth as well as high-speed interfaces. Katra city comprises 20 pedestrians and 6 stationary nodes having bluetooth interface only, 6 stationary nodes with the high-speed communication interface and 4 stationary nodes with both type of interfaces. 2 cars having high-speed interface and 2 cars with bluetooth interface are also placed randomly in Katra.

SMVDU comprises of 4 nodes as stationary node with bluetooth interface, 10 pedestrian nodes with bluetooth interface, 4 stationary nodes with the high-speed communication interface and 2 nodes kept stationary with both the interfaces. 2 cars with bluetooth interface and 2 cars with the high-speed interface. Reasi town comprises 20 pedestrians having bluetooth interface, 6 stationary nodes with bluetooth interface, 6 stationary nodes with the high-speed communication interface and 4 with both the interfaces, 2 car nodes having high-speed communication interface only and 2 car nodes having bluetooth interface only.

Fig 2. Experimental Scenario.

Akhnoor town comprises 20 pedestrian nodes, 2 car nodes and 6 stationary nodes (RSU) all having bluetooth interface. 6 stationary nodes (RSU) and 2 car nodes having high-speed communication interface but 4 car nodes with both the communication interfaces. Besides these, there are additional 20 cars and 8 stationary nodes having bluetooth interface only, 25 cars and 8 stationary nodes having high-speed interface only and 35 cars, 25 pedestrians and 4 stationary nodes having both are placed randomly in the whole bounded area. The nodes having both the interfaces i.e bluetooth interface and high-speed interface are gateways of the social skeleton model. The simulation setting parameters are listed in **Table 2**.

Table 2. Simulation Specification

Parameters	Value (Without Social Skeleton)	Value (With Social Skeleton)
Simulation Time	21600s	21600s
Interface	Bluetooth	Bluetooth
No of host groups	18	37
Number of Nodes	213	213
Routing Protocols	Epidemic, PRoPHET, Improved PRoPHET, Life Router, Spray and Wait,	Epidemic, Life Router, PRoPHET, Improved PRoPHET, Spray and Wait
Movement Model	Map Route Movement, Map Based Movement	MapRouteMovement, Mapbase Movement
Speed of Mobile Nodes	Pedestrian- 0.5-1.5 metre/second Car- 2.7-13.9 metre/second	Pedestrian- 0.5-1.5 metre/second Cars- 2.7-13.9 metre/second
Buffer Size	Stationary node buffer size: 1GB Mobile nodes buffer size: 5 MB	Stationary node buffer size: 1GB Mobile nodes buffer size: 5 MB
Size of Message	500KB -1 KB	500KB -1 KB
Time to live (TTL)	900 min	900 min
Event Generator used	Message Event Generator	Message Event Generator
Transmission range	Bluetooth: 10m	Bluetooth: 10m
Transmission speed	Bluetooth interface speed = 250kBps. High Speed Interface speed = 10MBps	Bluetooth interface speed = 250kBps. High-speed interface speed = 10MBps
World Size	100000 X 100000-metre square	100000 X 100000-metre square

Simulation Results and Analysis

ONE simulator is used to test the data routing in a proposed trust-based social skeleton. Data forwarding decision depends on the trust value of the node computed from the different parameters. In the simulation scenario the two parameters are considered i.e. contact frequency and number of packets forwarded. Two groups of nodes are created and considered as a social skeleton group and unsociable group. The results obtained after extensive simulation are compared with benchmark routing protocols without trust based social skeleton model. Delivery probability, overhead ratio and delivery delay are considered for evaluation of social skeleton performance.

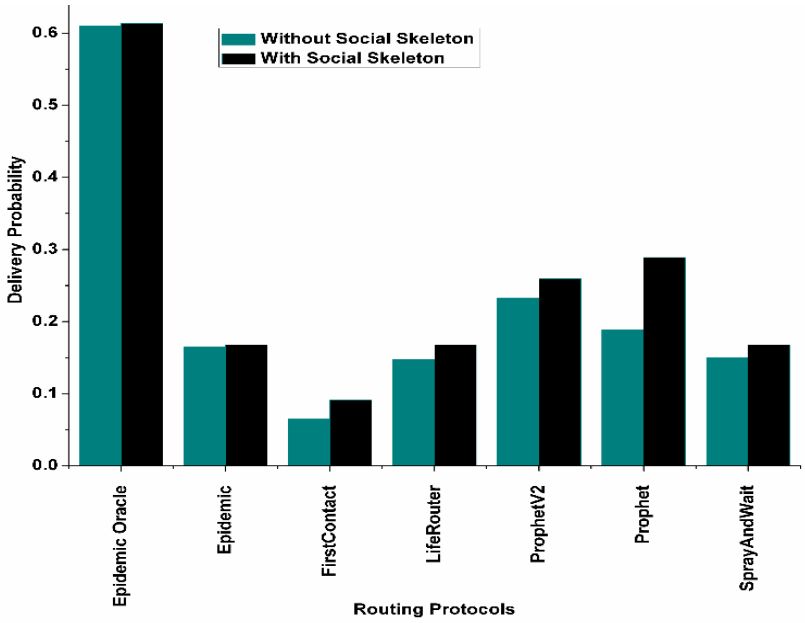

Fig 3. Delivery Probability vs. Routing Protocol.

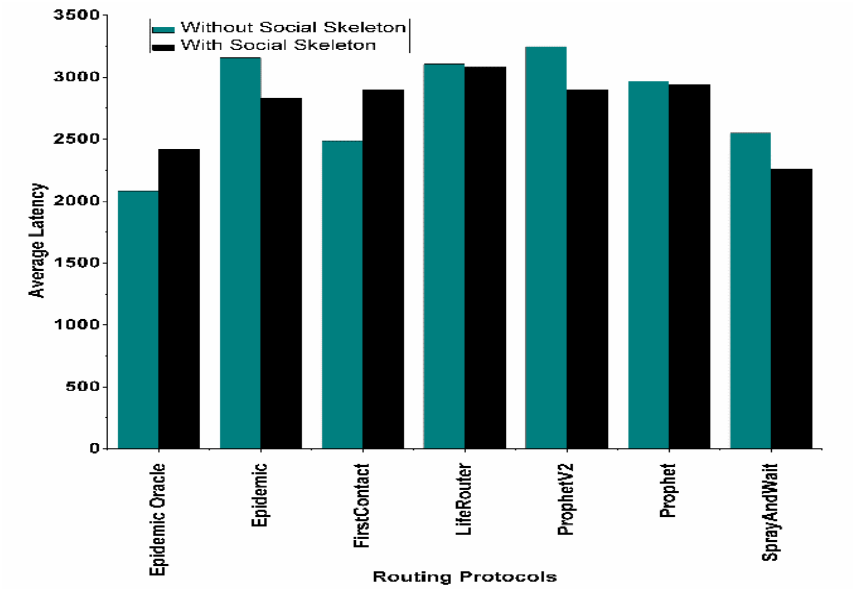

Fig 4. Average Latency vs. Routing Protocol.

Table 3. Delivery Probability vs Routing Protocols

Routing Protocols	**Delivery Probability**	
	Without Social Skeleton	**With Trusted Social Skeleton**
Epidemic Oracle	0.6106	0.6136
Epidemic	0.1652	0.1681
First Contact	0.0649	0.0914
Life Router	0.1475	0.1681
ProphetV2	0.233	0.2596
Prophet	0.1888	0.2891
Spray and Wait	0.1504	0.1681

Delivery Probability

Delivery Probability describes the value of sent packets over the packets created. It determines the probability of message delivery under a limited time interval. **Fig 3** and **Table 3** shows compared results for the delivery probability in case of social skeleton model. The Epidemic routing protocol outperforms in delivery probability in the social skeleton as well as in without social skeleton. However, the performance of Epidemic is better with social skeleton model. The performance of other routing schemes shows better performance with trusted social skeleton as compared to without social skeleton routing.

Table 4. Average Latency vs Routing Protocols

Routing Protocols	**Average Latency**	
	Without Social Skeleton	**With trusted Social Skeleton**
Epidemic Oracle	2081.6957	2422.3702
Epidemic	3156.5357	2831
First Contact	2486.4545	2901.451
Life Router	3106.9	3080.8246
ProphetV2	3248.3924	2900
Prophet	2969.75	2945
Spray and Wait	2549.9804	2257.8772

Average Latency

This factor determines the difference between the message creation time and its delivery time. **Fig 4** and **Table 4** depicts improved/comparable results for the proposed trust based social skeleton model. Epidemic oracle and first contact routing protocols having more average latency with social skeleton as compared to without social skeleton. Rest of all routing protocols exhibit less average latency as compare to without social skeleton.

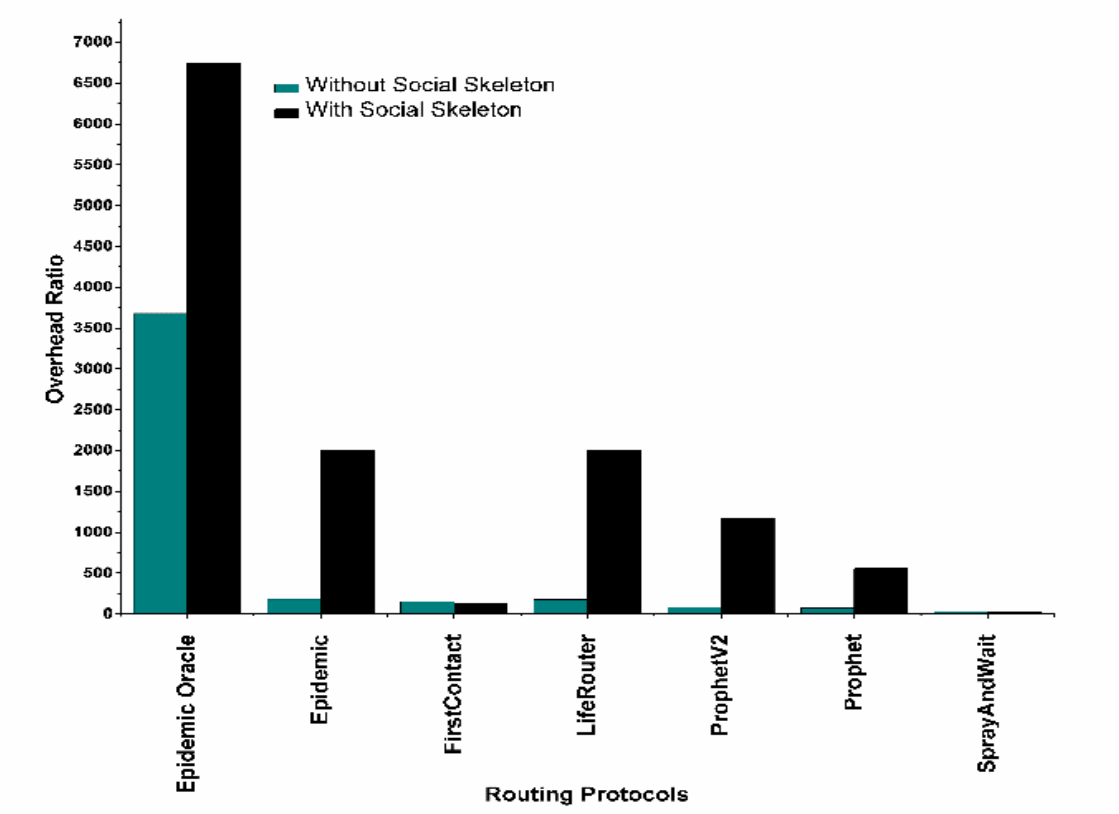

Fig 5. Overhead Ratio vs. Routing Protocol.

Table 5. Overhead Ratio vs Routing Protocols

Routing Protocols	**Overhead Ratio**	
	Without Social Skeleton	**With Trusted Social Skeleton**
Epidemic Oracle	3679.1691	6741.1442
Epidemic	180.16	2001.9825
First Contact	150.7273	126.7419
Life Router	176.44	2001.9825
ProphetV2	84.1899	1178.6136
Prophet	71.3594	559.1531
Spray and Wait	33.5641	28.6275

Overhead Ratio

Overhead Ratio defines as the number of extra copies of messages needed for the successful delivery of the message. It is determined by the ratio of remaining packets to the sent packets. **Fig 5** and **Table 5** shows compared results for the proposed trust based social skeleton model with more overhead ratio as compared to without social skeleton. In constrained resource scenarios the performance of social skeleton model can be low as compared to scenarios without a social skeleton. Overhead ratio is increased due to the exchange or replication of summary vectors to the neighbours.

VII. CONCLUSION

VDTN is the growing field with a considerable possibility to handle future requirements. Using vehicles for the communication purpose can be contemplated as a substitute for the wired and wireless systems. Research can be done in the areas of security, to maximize delivery, minimization of delivery delay with less utilization of resources.

In the present work, we have done analysis of the performance of VDTN in the presence of our proposed trust based social skeleton. The performance of the proposed social skeleton is being analysed and compared with benchmark routing protocols. The results show improved results for the delivery probability and comparable results for average latency and overhead ratio under the proposed social skeleton model because of data forwarding to the friend/trusted subset with the same social skeleton group.

Data Availability
No data was used to support this study.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
No funding agency is associated with this research.

Competing Interests
There are no competing interests

References

[1]. A. Sharma, N. Goyal, and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes," The Journal of Supercomputing, vol. 77, no. 6, pp. 6036–6055, Nov. 2020, doi: 10.1007/s11227-020-03507-4.
[2]. G. Santhana Devi and M. Germanus Alex, "DFEMD: Delay Tolerant Fast Emergency Message Dissemination Routing Protocol," Wireless Personal Communications, vol. 120, no. 4, pp. 3071–3093, Jul. 2021, doi: 10.1007/s11277-021-08600-2.
[3]. P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervello-Pastor, "From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks," IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 1166–1182, 2012, doi: 10.1109/surv.2011.081611.00102.
[4]. Haldorai, B. L. R, S. Murugan, and M. Balakrishnan, "AI-Based Effective Communication in Software-Defined VANET: A Study," EAI/Springer Innovations in Communication and Computing, pp. 271–290, 2024, doi: 10.1007/978-3-031-53972-5_14.
[5]. V. N. G. J. Soares, F. Farahmand, and J. J. P. C. Rodrigues, "A layered architecture for Vehicular Delay-Tolerant Networks," 2009 IEEE Symposium on Computers and Communications, Jul. 2009, doi: 10.1109/iscc.2009.5202332.
[6]. L. Li, X. Zhong, and Y. Qin, "A secure routing based on social trust in opportunistic networks," 2016 IEEE International Conference on Communication Systems (ICCS), Dec. 2016, doi: 10.1109/iccs.2016.7833575.
[7]. X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, "A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks," Peer-to-Peer Networking and Applications, vol. 10, no. 2, pp. 377–394, Feb. 2016, doi: 10.1007/s12083-016-0438-3.
[8]. V. Arulkumar, M. Aruna, D. Prakash, M. Amanullah, K. Somasundaram, and R. Thavasimuthu, "A novel cloud-assisted framework for consumer internet of things based on lanner swarm optimization algorithm in smart healthcare systems," Multimedia Tools and Applications, vol. 83, no. 26, pp. 68155–68179, Mar. 2024, doi: 10.1007/s11042-024-18846-0.
[9]. Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, "The Impact of Node Selfishness on Multicasting in Delay Tolerant Networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 5, pp. 2224–2238, 2011, doi: 10.1109/tvt.2011.2149552.
[10]. Y. Guo, S. Schildt, T. Pougel, S. Rottmann, and L. Wolf, "Mitigating Blackhole attacks in a hybrid VDTN," Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Jun. 2014, doi: 10.1109/wowmom.2014.6918993.
[11]. J. Golbeck and J. Hendler, "Inferring binary trust relationships in Web-based social networks," ACM Transactions on Internet Technology, vol. 6, no. 4, pp. 497–529, Nov. 2006, doi: 10.1145/1183463.1183470.
[12]. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," Proceedings 1996 IEEE Symposium on Security and Privacy, doi: 10.1109/secpri.1996.502679.
[13]. A. Baadache and A. Belmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1130–1139, May 2012, doi: 10.1016/j.jnca.2011.12.012.
[14]. S. E. Loudari, M. Benamar, and N. Benamar, "New Classification of Nodes Cooperation in Delay Tolerant Networks," Advances in Ubiquitous Networking, pp. 301–309, 2016, doi: 10.1007/978-981-287-990-5_24.
[15]. T. N. D. Pham, C. K. Yeo, N. Yanai, and T. Fujiwara, "Detecting Flooding Attack and Accommodating Burst Traffic in Delay-Tolerant Networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 1, pp. 795–808, Jan. 2018, doi: 10.1109/tvt.2017.2748345.
[16]. J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A Cooperative Watchdog System to Detect Misbehavior Nodes in Vehicular Delay-Tolerant Networks," IEEE Transactions on Industrial Electronics, vol. 62, no. 12, pp. 7929–7937, Dec. 2015, doi: 10.1109/tie.2015.2425357.
[17]. Q. Li, W. Gao, S. Zhu, and G. Cao, "To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 3, pp. 168–182, May 2013, doi: 10.1109/tdsc.2012.84.
[18]. M. Y. S. Uddin, B. Godfrey, and T. Abdelzaher, "RELICS: In-network realization of incentives to combat selfishness in DTNs," The 18th IEEE International Conference on Network Protocols, Oct. 2010, doi: 10.1109/icnp.2010.5762769.
[19]. 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, no. 9, pp. 1514–1531, Sep. 2012, doi: 10.1109/tmc.2011.160.
[20]. Haojin Zhu, Xiaodong Lin, Rongxing Lu, Yanfei Fan, and Xuemin Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Transactions on Vehicular Technology, vol. 58, no. 8, pp. 4628–4639, Oct. 2009, doi: 10.1109/tvt.2009.2020105.
[21]. H. Gong, L. Yu, and X. Zhang, "Social Contribution-Based Routing Protocol for Vehicular Network with Selfish Nodes," International Journal of Distributed Sensor Networks, vol. 10, no. 4, p. 753024, Apr. 2014, doi: 10.1155/2014/753024.
[22]. L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," Ad Hoc Networks, vol. 8, no. 1, pp. 1–14, Jan. 2010, doi: 10.1016/j.adhoc.2009.02.005.
[23]. F. Wu, T. Chen, S. Zhong, C. Qiao, and G. Chen, "A bargaining-based approach for incentive-compatible message forwarding in opportunistic networks," 2012 IEEE International Conference on Communications (ICC), Jun. 2012, doi: 10.1109/icc.2012.6363685.
[24]. L. Liu, "A survey on barter-based incentive mechanism in opportunistic networks," 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), Dec. 2013, doi: 10.1109/imsna.2013.6743291.
[25]. A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," Proceedings of the Second International ICST Conference on Simulation Tools and Techniques, 2009, doi: 10.4108/icst.simutools2009.5674.