Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 7353691, 18 pages
http://dx.doi.org/10.1155/2016/7353691

*Research Article*

# Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN

**Jan Papaj and Lubomir Dobos**

*Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Kosice, Letna 9, 042 00 Kosice, Slovakia*

Correspondence should be addressed to Jan Papaj; jan.papaj@tuke.sk

Received 4 January 2016; Revised 8 March 2016; Accepted 23 March 2016

Academic Editor: Ioannis Papapanagiotou



Today's mobile networks require integration of the different networks in order to transport data between mobile devices. The main problems of all networks occur if the communication paths are disconnected for a short time. The hybrid MANET-DTN is an evolution of the Mobile Ad Hoc Networks (MANET) and Delay/Disruption Tolerant Network (DTN) and it gives the possibilities of data transport between the disconnected islands of the nodes. The key problem is how to select reliable and secure nodes to transport messages between isolated islands with limited connectivity. The selection of the relay nodes is a critical factor because the data are transported via these devices in hostile environments. Two algorithms for a relay node selection based on trust are introduced. These algorithms are activated if the connections are disrupted. The selected relay nodes transport data across the disconnected environment via store-carry-forward mode. The proposed algorithms enable selecting reliable relay nodes based on collecting routing information and contact history. We introduce the network performance analyses of these algorithms. The main idea of the analyses is studying how the algorithms can affect the behaviour of the routing and forwarding mechanisms in the simulator OPNET modeler.

## 1. Introduction

A new concept of the hybrid MANET-DTN enables a progressive and robust communication between mobile terminals in the hostile and disconnected environment. This network enables integration of the Mobile Ad Hoc Network (MANET) for situations when mobile nodes can communicate with each other via wireless links and Delay/Disruption Tolerant Network (DTN) in the case when the communication paths never exist or the signal between mobile terminals is weak. This network integrates the benefits of the MANET routing algorithm for transmitting the data and DTN forwarding technique in order to obtain transportation path between a source and destination terminals.

The Mobile Ad Hoc Network (MANET) is characterized by multihop communication between mobile nodes by wireless links [1]. There are also no infrastructures and routing paths are established by routing algorithms (Figure 1). The traditional routing algorithms and protocols are based on routing schemes, which can find a path for a given node pair according to various metrics, and data packets are transmitted from one intermediate relay node to the next specified relay based on physical condition of wireless channels [2]. The routing algorithm relies on the assumption that the network graph is fully connected and fails to route messages if there is no complete route from source to destination at the time of sending [3]. The key mechanism is the routing protocol that allows finding a path for a given node pair (source and destination node) according to various metrics. The routing protocols and algorithms can be classified into three categories: reactive, proactive, and hybrid [1, 2, 4].

The Delay/Disruption Tolerant Networks (DTN) have been developed for intermittent communication between mobile terminals. The main feature of these networks is high propagation delays when transferring data between different terminals. DTN provides high bit error rates and the long-term disconnections experienced in such environments. DTN is proposed and designed to operate in hostile

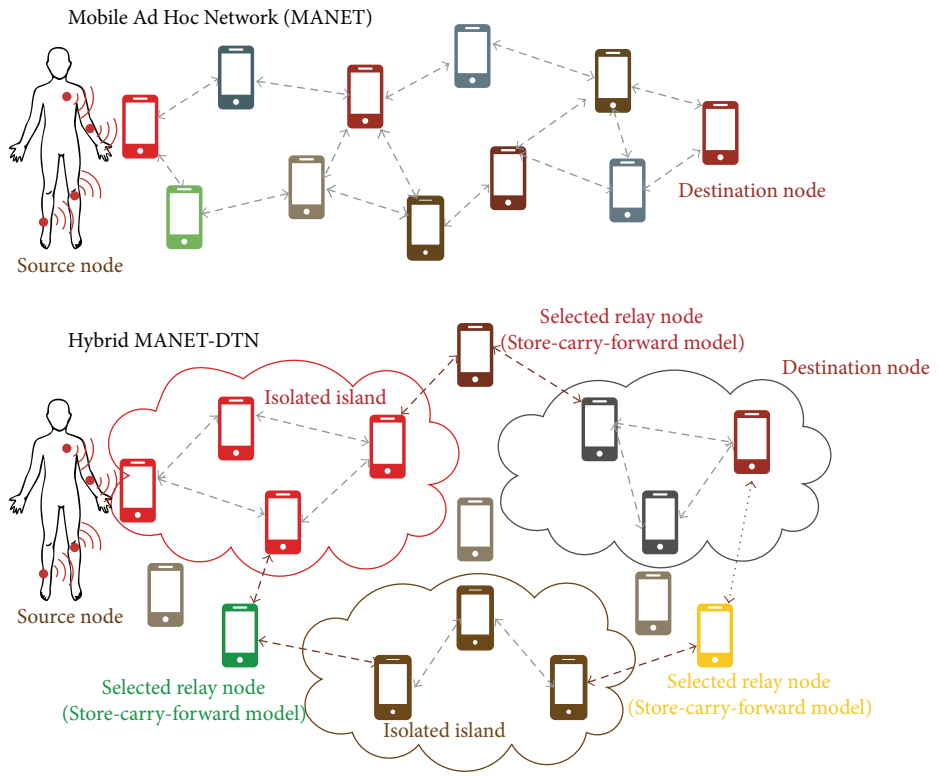



Figure 1: Example of the MANET and hybrid MANET-DTN.

environments. DTN is characterized by very long delay paths and frequent network partitions [5–7]. DTN consists of human-carried mobile devices (smartphones, PDA, etc.) that communicate with each other without mobile or fixed infrastructure. DTN forwarding algorithms allow sending messages via the broadcast nature and spatial diversity of the wireless medium. Forwarding algorithms use the store-carry-forward model and are based on stochastic approach.

Security is a key field for all types of network, not only in MANET, DTN, or hybrid MANET-DTN [8, 9]. In MANET, the security mechanisms are based on the assumption that there are connections between a source and target nodes (end-to-end connections) [2]. In DTN, we require the security solutions, which provide security for all nodes, all services, and application that participate in routing and transmitting process. Based on a sporadic connectivity of nodes, it is necessary to provide secure delivery of the messages from the source node to the destination node. The hybrid MANET-DTN integrates security issues from both types of networks and provides more challenges to solve security problems.

*1.1. Relay Node Selection and Main Motivation in Hybrid MANET-DTN.* In order to provide the effective communication between isolated islands of mobile nodes or between disconnected mobile nodes, it is necessary to consider different aspects such as disconnections, mobility, partitions, environment, and norms instead of the exceptions. The mobility in DTN is used to provide efficient communication between unconnected groups of nodes (isolated islands). The mobile nodes forward data and also store data in the cache for a long time. This model is called store-carry-forward [2].

The selection of forwarding relay node is the first key issue. There are few works which deal with the selection of the relay nodes. The first access is based on the number of transitions (Expected Transmission Count (ETX), Expected Any-Path Transmission (EAX)) which accounts for the specific characteristics of the opportunistic paradigm [10]. Other algorithms are based on a link-state algorithm for the unconstrained selection based on the Dijkstra algorithm [11]. Most methods are based on generalizing the Bellman-Ford algorithm and they prove its optimality [12, 13].

The hybrid MANET-DTN also requires the cooperation between mobile terminals in order to make a selection of the relay nodes. Relay nodes are nodes that have a higher probability of connecting with other nodes or allowing the transmission of the messages by wireless environment. Selection of the relay nodes is made opportunistically based on an actual network environment. There is very little research on the relay node selection for hybrid MANET-DTN due to the many additional challenges that they face in comparison with traditional MANET or DTN.

In this paper, the novel trust based relay node selection algorithms are introduced. These mechanisms enable selection of the secure mobile node used for transportation of the data across the disconnected environment. Selected relay nodes provide the secure mobile node selected to transport the data. If the mobile node finds a connection

the DTN forwarding mechanism is activated. The proposed mechanisms also provide wide challenges for new services not only for emergency situations.

*1.2. Trust in Hybrid MANET-DTN.* The term trust can be reflected by reliability, utilization, availability, reputation, risk, confidence, quality of services, and other concepts [4]. Trust is targeting various scientific disciplines, such as sociology, economics, management, and informatics. In each of these sectors, the trust is defined differently for a specific type of use or focus in that area. For example, in sociology trust is represented as a relationship in nature [14, 15], but in psychology it is trust in a meaning of a personal attribute view. When we apply trust to MANET or even to newer hybrid MANET-DTN we can classify trust into the following four categories [16]:

(i) *Trust as a risk factor*: The definition says that if an individual node decides to send data through ambiguous path favourable and unfavourable state may occur. This condition depends on future actions of the recipient. The parameter trust can be used as a prediction of the future behaviour of other nodes.

(ii) *Trust as a belief*: Trust is understood as an individual faith in the behaviour of nodes based on their previous actions and decisions.

(iii) *Trust relationship with transitivity*: Trust is a weighted binary relationship between two nodes in the network. As an example here we can mention hierarchically constructed network, where node $A$, which is higher in the hierarchy, may decide to send data to node $B$, which is lower in the hierarchy, whether it is trusted or untrusted.

(iv) *Confidentiality as a subjective probability*: Trust is the probability level determined on the basis of subjective decision-making, where a node determines the value of the likelihood with which monitored node takes certain action at a certain time and in a specified context.

We can summarize these definitions as a trust for a particular node in the network is a subjective assessment of the agent or other nodes on the reliability and accuracy of received and sent information through this node in a given context. Trust reflects a belief or expectations for reliability, availability, integrity, and quality of service of target node from the perspective of future activity and behaviour of that node.

We determine the metric based on various input parameters and based on this metric we are able to determine the value of trust. The metric can be classified into three basic categories [14]:

(i) *Scale model*: In this sense trust is computed with discrete confidentiality or continuous values to some extent and a predetermined threshold is used for comparison and evaluation.

(ii) *Facets model*: The model is defined as certainty (confidence) and confidentiality to the same extent as $\langle 0, 1\rangle$ and together they represent credibility (trustworthiness). This trustworthiness can be shown as the shortest distance from the start to the point with coordinates (confidentiality, integrity) in 2D space. Metrics may also be composed of several values; for example, $b + d + u = 1$, where $b$ is the belief, $d$ is disbelief, and $u$ is uncertainty. Trust is then represented in this space.

(iii) *Fuzzy model*: Some approaches use probability as a metric for determining confidentiality. Bayes statistics are used as a parameter entering into the calculation of this probability. Another parameter can be, for example, a number of received packets, a number of failed packets, and a number of interactions.

In general, trust is a relative term and it is possible to assign to it different values based on a specific proposal for its computation. For example, the trust can be assigned values of the interval $\langle -1, 1\rangle$, where $-1$ represents the complete untrusted $+1$ opposite.

In hybrid MANET-DTN, the key aspect is how these trust concepts can be applied to modeling trust [4, 15, 17–19]. Trust for a particular node in the network is a subjective assessment of the agent or other nodes on the reliability and accuracy of received and sent information through this node in a given context [15]. In this work, we are focused on direct trust calculation (see Figure 2).

## 2. Novel Relay Node Selection Algorithms in Hybrid MANET-DTN

The main idea of the algorithms is providing relevant and innovative information, which will be used for selecting of the trusted relay nodes. These nodes will be used for transportation of the data messages between isolated terminals or isolated islands of the mobile terminals. Algorithms integrate monitoring of the networks for collecting of the data used for trust computing. The main ideas for all models are displayed in Figure 3.

Proposed models are based on the direct model for the trust computation. Models are also based on the assumption that each node in the network receives information about other nodes. The collected data are stored in each node and later used in the calculation of the preliminary and final values of trust, which are used for selection of the relay nodes. The proposed algorithm is working on the network layer of the MANET layer model and is designed for collecting of the routing and data node information throughout the entire operations specified for the routing.

*2.1. Designed Relay Node Selection Algorithms in Hybrid MANET-DTN.* As we mentioned before, the first algorithm enables monitoring of the routing process in the MANET and DTN environment. Figure 4 shows the main idea and the flow diagram of the proposed algorithm for calculation of trust

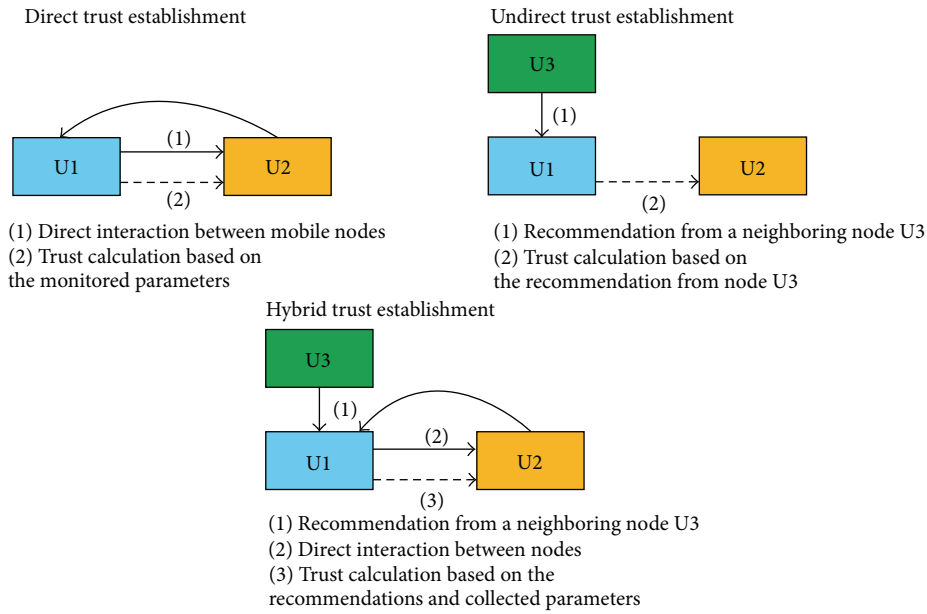



Figure 2: Three basic models for trust computation used for hybrid MANET-DTN.

and selection of the relay nodes. The algorithm can be divided into two main phases [4]:

(i) Phase of obtaining and storing information.

(ii) Phase of trust computing.

These phases are carried out whenever the packet is received by the node. It is for this reason that the final value of the trust is always up to date and it makes changes dynamically, as well as changing the network topology, which is related to the mobility of nodes. The final value of the trust reflects the current state of the parameters obtained from the network [4].

*2.1.1. Phase of Obtaining and Storing Information.* The algorithm for the trust calculation is triggered whenever a change occurs in the obtained parameters. The routing packet coming from the lower layer (physical and data link layer) is encapsulated and the network layer is an IP packet containing different information [4].

The one such important piece of information is collected from the routing packets (DSR reactive routing protocol). This information tells what kind of packet goes. In the proposed algorithm, the incoming packets are used as parameters which enter into the final calculation of trust and the following parameters are used for calculation: a total number of route request packets received at node, a total number of route reply packets received at node, a total number of route error packets received at node, a total number of route acknowledgement packets received at the node, a total number of data packets received at node, a number of route requests received from each node, a number of route replies received from each node, a number of path errors received from each node, number of route replies received from each node, and number of data packets received from each node.

The data from this phase are stored in the data structure in memory on each node separately. Each node stores information about nodes with whom it came in contact. The algorithms also exchange routing information or data traffic between each other. Each node in the network is independent and has the possibility of calculating the final value of trust to the other node. Information is stored in a format which has the form of a table and is available during the time when the node is part of the network. After this time, the values will be set up to the minimum that means they will be marked as untrusted. This structure is dynamic and its size can vary based on the number of nodes with which node communicates [4].

Figure 5 illustrates the phase of obtaining and saving parameters and we can see four communicating nodes ID_1, ID_2, ID_3, and ID_4. In this scenario, node ID_1 sends a packet type route request to node ID_4 and node ID_2 sends a route error packet to node ID_3. From a node ID_4 point of view, node updates the parameter table and stores new values into the structure. That structure is dynamic in size because it is not known in advance how many nodes in the network can be located and how many nodes can communicate with this node [4].

*2.1.2. Phase of Trust Parameter Computing Trust.* After retrieving and updating the parameters in the table of parameters for each node, it is necessary to calculate and update the value of trust. At this stage, the value of the trust is calculated from the obtained parameters. Computing of trust is based on the direct model for the calculation of trust. This means that the resulting value was not sent further to other nodes as a recommendation and it serves locally on that node and helps

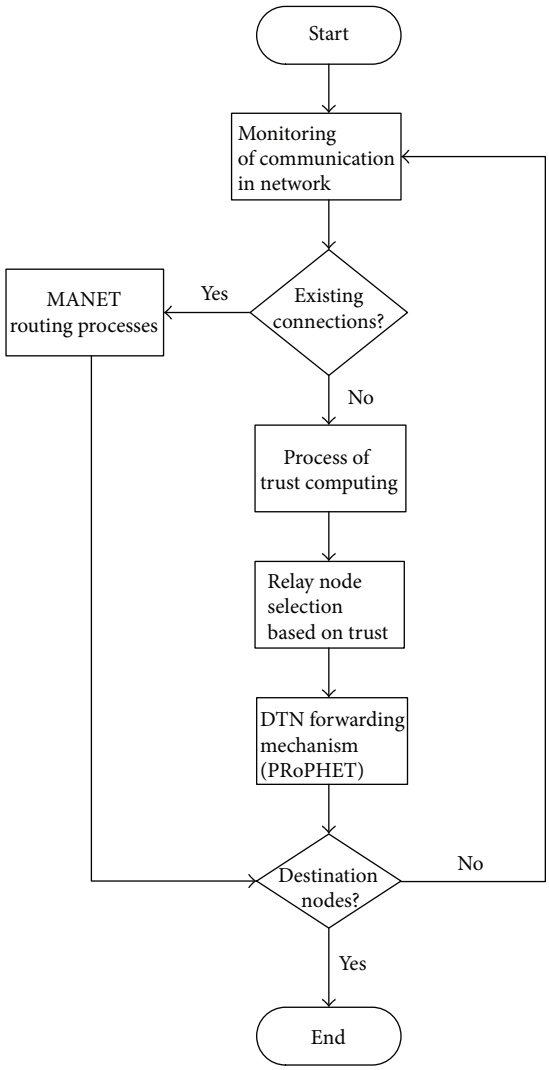



Figure 3: The main idea of the new algorithms for the relay nodes selection in hybrid MANET-DTN.

the node to decide during relay node selection. In our case, the calculated value of thrust will be used as a one parameter for the selection of the relay node or nodes in a situation where there is a disconnection in the network and the node will not have a backup path to the destination node (Figure 6). The actual calculation of trust can be divided into two parts [4]:

(i) *Trust calculation from routing information* $T_s$: it gives information about how the trust will be affected by the routing activities on the given node.

(ii) *Trust calculation from data packets* $T_d$: it gives information about how the data transmission (without routing packets) can affect the trust on the given node.

From these two subcalculations we get the final value of trust $T$, which is registered and stored in each node data structure. Analyses of individual fragment values are given in

$$T_s = W_{\mathrm{RREQ}} * \left(\frac{R_{\mathrm{REQ}}}{R_{\mathrm{REQT}}}\right) + W_{\mathrm{RREP}} * \left(\frac{R_{\mathrm{REP}}}{R_{\mathrm{REPT}}}\right) + W_{\mathrm{RERR}} * \left(\frac{R_{\mathrm{RERR}}}{R_{\mathrm{RERRT}}}\right) + W_{\mathrm{RACK}} * \left(\frac{R_{\mathrm{RACK}}}{R_{\mathrm{RACKT}}}\right),$$
$$T_d = W_d * \left(\frac{D}{D_t}\right), \tag{1}$$

where $T_s$ and $T_d$ are mentioned partial trust values computed from routing and data traffic on given node. The values $T_s$, $T_d$, and $T$ will be updated after the packets will be received. If a new mobile node will be in a network, the algorithm assigns the node as a node with the minimum value of trust and, from this time, the values of the trust will be computed and updated.

Furthermore $W_{\mathrm{RREQ}}$, $W_{\mathrm{RREP}}$, $W_{\mathrm{RERR}}$, $W_{\mathrm{RACK}}$, and $W_d$ are constants, which define a weight of trust value, and that resulting value will be in the selected range. Constants can be changed based on the types of attacks and on the basis of what we want to balance with the individual parameters entering into the calculation of trust. The values in the numerator of the equation represent the number of packets of each type from specific nodes in the network. Values $R_{\mathrm{RREQT}}$, $R_{\mathrm{RREPT}}$, $R_{\mathrm{RERRT}}$, $R_{\mathrm{RACKT}}$, and $D_t$ represent the total number of packets from all nodes received on the given node and $R_{\mathrm{RREQ}}$, $R_{\mathrm{RREP}}$, $R_{\mathrm{RERR}}$, $R_{\mathrm{RACK}}$, and $D$ are the values of the specific packets received from a given node. The value representing final value of trust $T$ is shown in

$$T = T_s + T_d, \tag{2}$$

where $T_s$ and $T_d$ values are partial trust mentioned above. The nodes with higher value of these parameters are selected as a secure relay node for transportation messages between isolated islands (see Figure 1).

*2.2. Enhancement of the Algorithm for Selection of the Relay Node in Hybrid MANET-DTN.* The main idea of this algorithm is also displayed in Figures 3 and 7. It is an extension of the previous model (see Section 2.1). The values of trust computed from formula (2) are stored in memory and they are available for selection of the trusted nodes for the case that newly computed values of trust are inadequate.

The extension and enhancement are based on using of the parameter trust that is obtained from the history of contacts. Specifically, the parameters *number of transmissions* and *length of transmission* are used for selecting of the relay node. Values of these parameters will be obtained during direct communication with other mobile nodes. The number of transfers will be evaluated from incoming and outgoing routing packets. The length of the transmission will be evaluated only from the received packet and it will be available during a time when a node is part of the network.

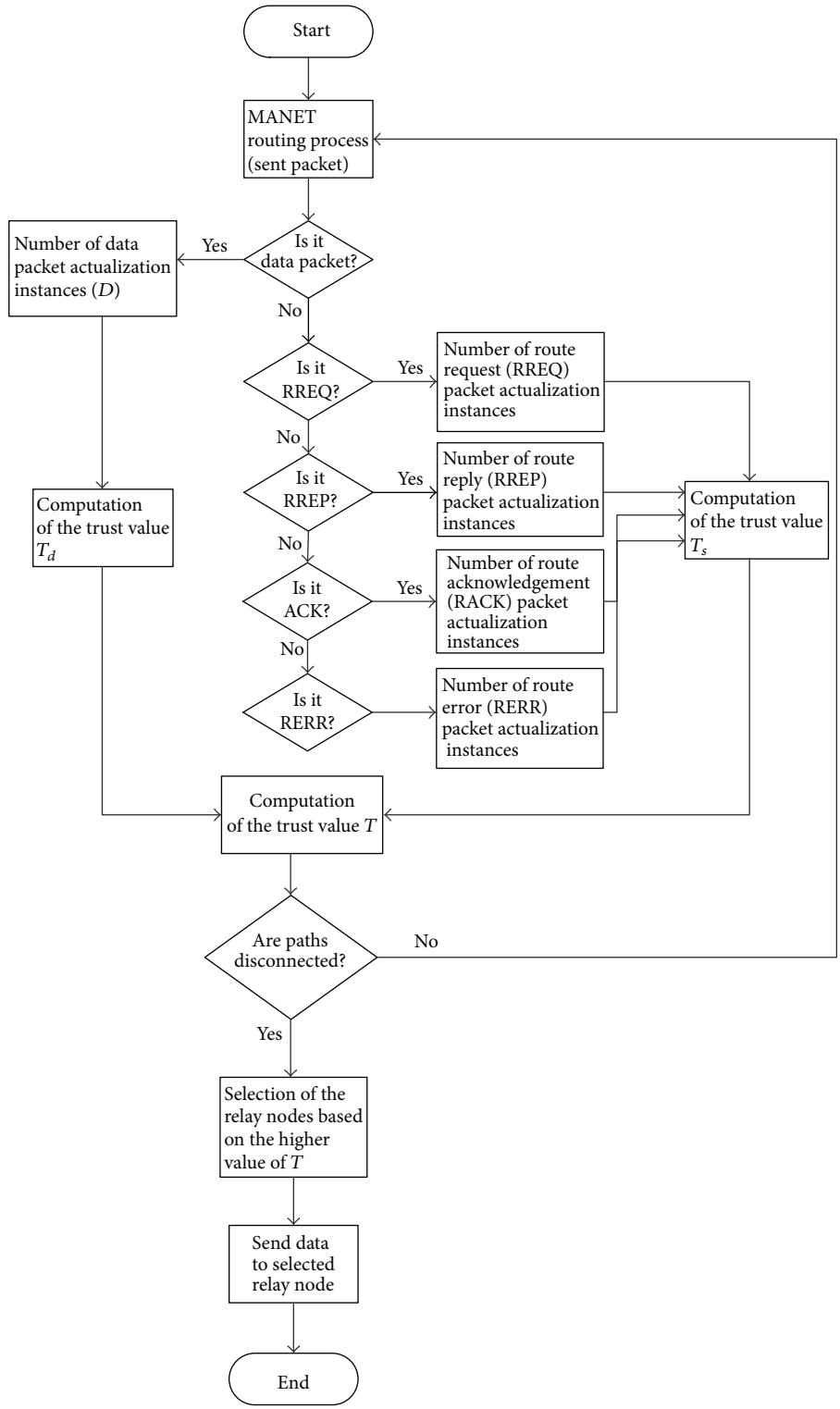
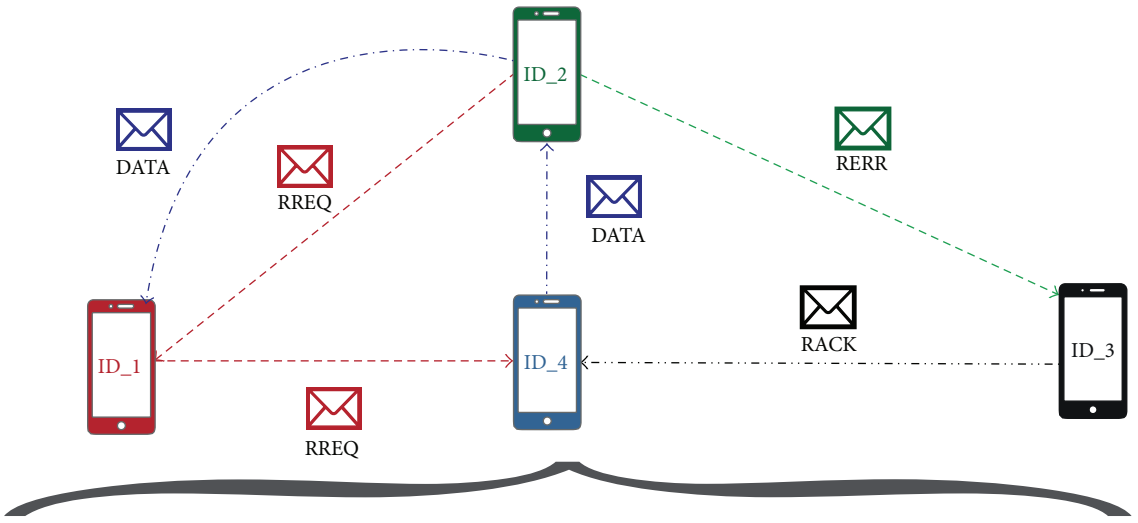



Figure 4: The flowchart of the algorithm for hybrid MANET-DTN.

In this enhancement of the algorithm, the direct trust computation is applied, too. It means that the trust is calculated based on the parameters which itself acquired and which relate to the neighbor nodes. The advantage of this approach lies in the fact that the trust reflects the views only for the actual node and it cannot be distorted by malicious nodes. The disadvantage is the loss of a number of values about the trust of the node, resulting in the loss of objectivity in evaluating the trust. The modification relies on the following steps:




| Node ID | RREQ | | RREP | | RERR | | RACK | | DATA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Received | Total | Received | Total | Received | Total | Received | Total | Received | Sent | Trust |
| ID_1 | 128 + 1 | 234 | 87 | 147 + 1 | 12 | 25 | 82 | 548 + 1 | 2467 + 1 | 1228 | −0,816 |
| ID_2 | 475 | 268 + 1 | 24 | 88 | 13 | 29 + 1 | 124 + 1 | 265 | 2674 + 1 | 4325 + 1 | 0,426 |
| ... | | | | | | | | | | | |

Figure 5: Collecting of the routing data for trust computing in hybrid MANET-DTN.

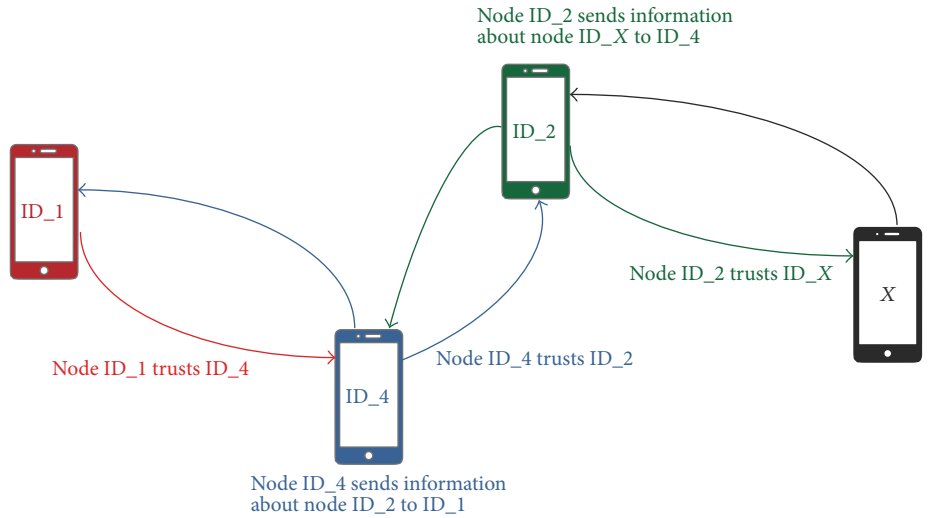



Figure 6: Promotion calculated value of the trust between nodes during computing of the trust in hybrid MANET-DTN.

(i) Phase of initialization and obtaining the values of number of transmissions and length of transmission for trust computing in hybrid MANET-DTN.

(ii) Phase of trust computing for a relay node selection.

*2.2.1. Phases of Initialization and Obtaining the Values of Number of Transmissions and Length of Transmission for Trust Computing in Hybrid MANET-DTN. Initialization phase* deals with establishing of the parameter table, where the meeting records of nodes together with the values of monitoring parameters as the value of the trust will be recorded. There will be also the variables which will hold the value of each parameter involved in the calculation of the trust, namely,

(i) the identifier of the current node (AU),

(ii) the identifier of the previous node (PU),

(iii) the time of creation of the packet (CV),

(iv) the time of receipt of the packet (CP),

(v) the length of the current transmission DP (difference between CP and CV),

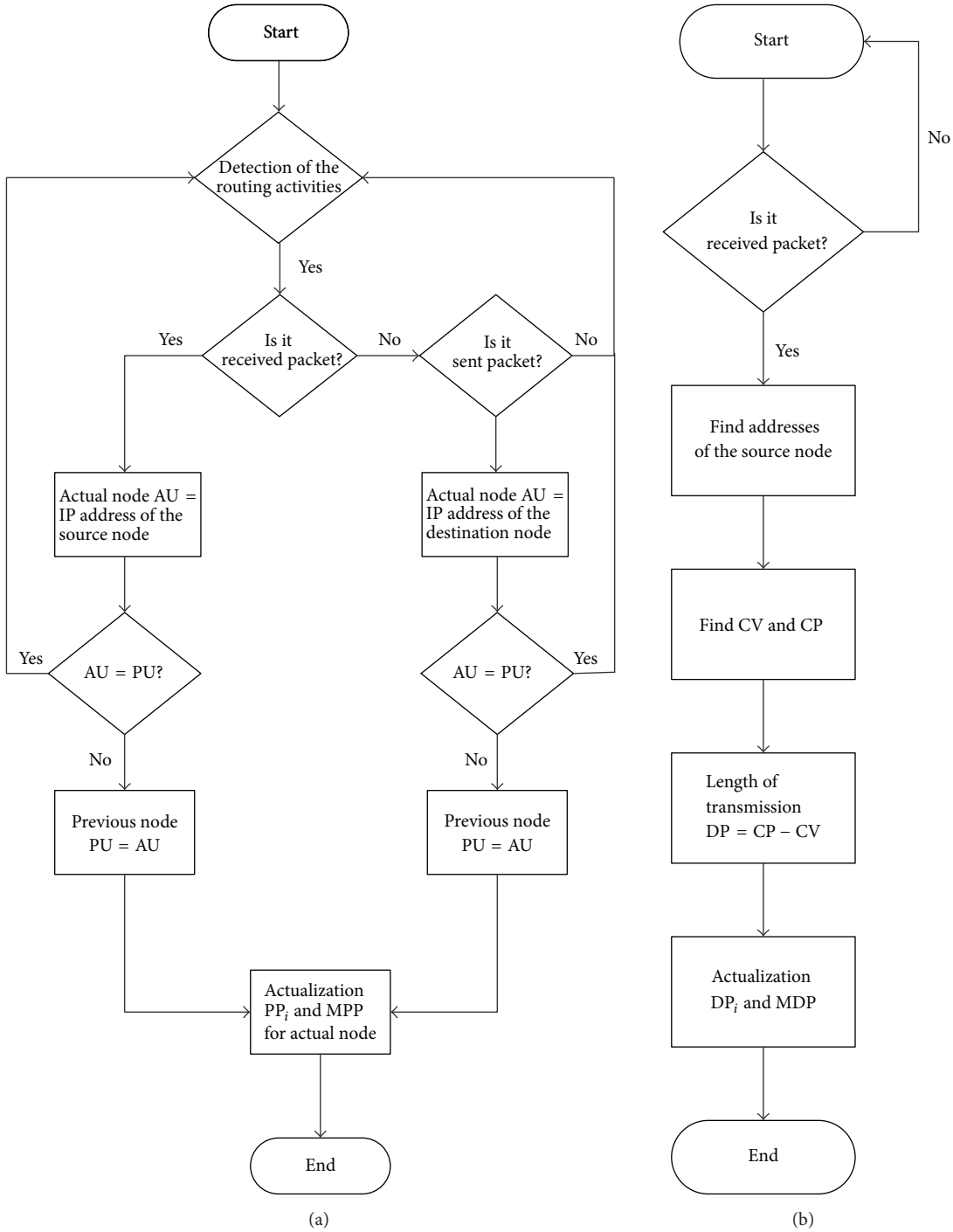



Figure 7: Flowchart for collecting parameters: (a) number of transmissions and (b) length of the transmission in hybrid MANET-DTN.

(vi) parameter number of transmissions between the $i$-nodes ($PP_i$),

(vii) length of transmission between $i$th nodes ($DP_i$),

(viii) maximum number of transmissions with nodes (MPP),

(ix) maximum transmission distance among all nodes (MDP),

(x) the length of the current transmission DP (difference between CP and CV),

(xi) parameter number of transmissions between the $i$-nodes ($PP_i$),

(xii) normalized number of transfers with the $i$-node ($NPP_i$),

(xiii) standardized transmission distance of the $i$-node ($NDP_i$),

(xiv) weight for standardized number of transmissions ($W_p$),

(xv) weight for standard length ($W_d$),

(xvi) transfers and the value of confidentiality for the $i$-node ($T_i$).

The *number of transmissions* is obtained from incoming and outgoing routing packets and it represents the number and frequency of the meetings with other mobile nodes (see Figure 7(a)). It is the most fundamental parameter history of meetings and gives an approximate view of the relationship between nodes. The value of this parameter depends on the number of packets sent and received between two nodes. The proposed algorithm enables determining routing activity in the network; it means that node received or sent packets. If there is no activity, the phase of initialization is activated and algorithm waits for the routing transmission. If there are detected routing activities, node identifier in the form of an IP address is stored in the variable AU into the current node; then the algorithm compares the current identifier to distinguish whether it is a new transmission or only the transmission of multiple packets to one goal. If this is a new transfer, it updates the value of the number of transmissions for the $i$-node based on the IP address. It also updates the value of the total number of transmissions and the total number of times of all nodes. Finally, the IP address as an identifier of the previous node is inserted into the variable for the previous node PU and the algorithm is terminated, respectively, and enters the initial state.

At the same time, the length of the transmission is activated (see Figure 7(b)). This parameter is an extension of the parameter number of transmissions and gives a better view of the history of contacts. The combination of these parameters allows defining precisely the relationship between two nodes and also the trust. If a packet is received, it is found which node was the sender of the packet; then the variable value CV puts the time when the packet was created. The variable time of receipt CP is inserting time data when a packet has been received. From the last two parameters DP can be calculated as the difference between the received time and time of creation of the packet. This value should be added to a specific $DP_i$ value in the table of parameters. All $DP_i$ values are compared in the nodes and a maximum value of transmission MDP will be used as the highest value. Finally, the algorithm will go into the initial state again or stop and will wait for incoming packet transfer. After obtaining these parameter values, an algorithm calculates the value of trust. This value will reflect the view of one node to another, and trust will be used to select a trusted relay node.

*2.2.2. Phase of Trust Computing for a Relay Node Selection.* Based on collected values mentioned in Section 2.2.1, the algorithm for trust computing is activated. The values of these parameters are updated whenever the packets are received, or sent (Figure 8); in this way, the trust value updates the actual state of the network. Each mobile node has stored information about number and length of transmissions. These values are computed as

$$\begin{aligned} \mathrm{MPP} &= \max_n \sum \mathrm{PP}_i, \\ \mathrm{MDP} &= \max_n \sum \mathrm{DP}_i, \end{aligned} \tag{3}$$

where $i$ is order of the node and $n$ is number of the nodes. All these values are normalized by the following formulas:

$$\begin{aligned} \mathrm{MPP}_i &= \frac{\mathrm{PP}_i}{\mathrm{MPP}}, \\ \mathrm{MDP}_i &= \frac{\mathrm{DP}_i}{\mathrm{MDP}}. \end{aligned} \tag{4}$$

After normalization, the values will be in the range between 0 and 1. At the same time, each value of describing a relationship or proportion of the total, respectively, is maximum value. This ensures the relevance of each value for each parameter will reflect the relationship between the actual state history meetings. After this step, the process of weighting is applied. The weights are given information about the importance of this parameter and it is in the range $\langle 0, 1 \rangle$ and the total sum of values is equal to 1. The total values of the trust for each mobile node are then computed by the following formula:

$$T_i = W_p * \mathrm{NPP}_i + W_d * \mathrm{NDP}_i, \tag{5}$$

where

$$W_p + W_d = 1. \tag{6}$$

As we mentioned the given algorithm is an extension of the algorithm described in Section 2.1. After computing of the value trust, the values of $T_i$ will be compared with stored values $T$ collected during the first stage (Section 2.1) and the trusted relay node is selected as a node with a maximal number of trust values.

## 3. Simulations and Results

The main objective of simulations is to analyse how the proposed algorithms can affect the behaviour of the network in the sense of the network performance. As a simulation tool, the OPNET modeler simulator [20] was used for testing of the proposed mechanisms. OPNET provides a lot of useful tools for analysing of the mobile networks and enables simulating MANET with different routing protocol as well [1]. The Dynamic Source Routing protocol was used for testing and the collected values represent a reference value for analysing of the behaviour of the MANET [1].

Moreover, we have implemented the PRoPHET forwarding mechanism based on the history of past encounters (Figure 9) [20]. This algorithm enables simulation of the DTN in OPNET modeler. The implementation allows simulating cases based on the bundle concept as epidemic forwarding and the routing algorithm based on the history of past encounters. PRoPHET is specifically intended to provide

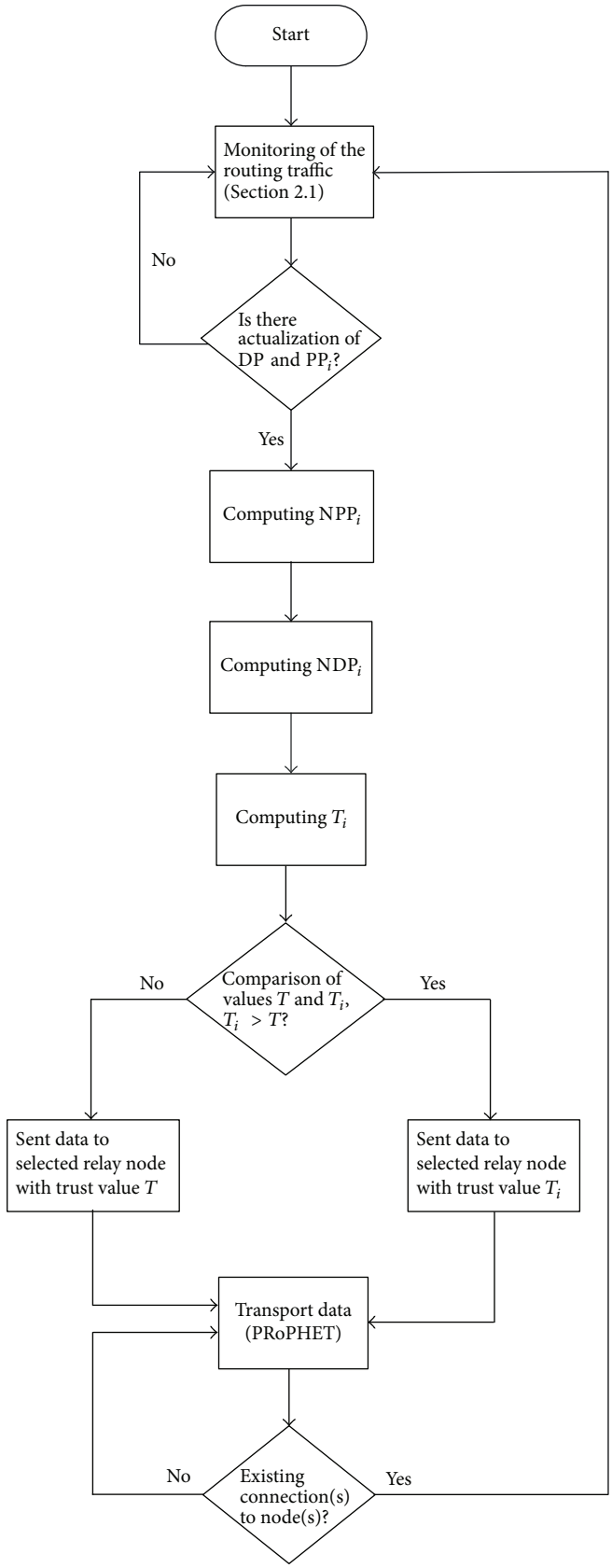



Figure 8: Process of the trust computing in hybrid MANET-DTN.

Table 1: Simulation setup for OPNET modeler.

| Parameters | Values |
|---|---|
| Simulation area | 2000 m × 2000 m |
| Simulation time | 1000 s |
| Transmission range | 250 m |
| Transmitted power | 1 mW |
| Type of service | CBR |
| Number of nodes | 20, 40, 60, 80, 100 |
| Speed of nodes | 0–6 m/s |
| Mobility model | Mobility model Default Random Waypoint |
| Nodes location | Random |
| Pause time | 10 s |
| Simulation runs | 100 |
| Number of values per simulation | 1000 |
| Reference values of trust | $W_{\text{RREQ}} = 0.2, W_{\text{RREP}} = 0.5, W_{\text{RERR}} = 0.2, W_{\text{RACK}} = 0.2, W_d = 0.3, W_p = 0.7$ |

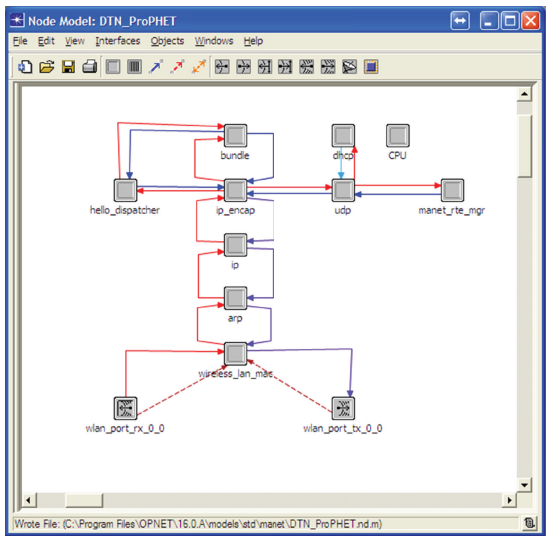



Figure 9: PRoPHET forwarding model for DTN in OPNET modeler.

routing services in a bundle network environment. It is mentioned that the PRoPHET is defined to run over reliable TCP, the submessages are provided with sequence numbers, and this, together with a capability for positive, would allow PRoPHET to operate over an unreliable protocol such as UDP or directly over IP [21, 22].

In order to check the functionality of the proposed algorithms, the following simulation scenarios were used to analyse the network performance of the proposed mechanisms:

(i) *MANET model (DSR)*: MANET used standard DSR protocol without the possibility of finding communication paths between mobile nodes if there are disconnections.

(ii) *MANET model with TRUST (DSR_TRUST1)*: it is MANET with DSR protocol. The possibility of finding a secure relay node based on trust is implemented (see Section 2.1).

(iii) *MANET model with TRUST (DSR_TRUST2)*: it is enhanced version of model DSR_TRUST1 (see Section 2.2).

(iv) *DTN model (DTN)*: it is extension of model DSR_TRUST2 with the PRoPHET protocol. This model enables finding a communication path via *store-carry-forward* model if the communication links are disconnected during the transportation of the packets.

The simulation setup and parameters for the OPNET modeler are summarized in Table 1. During simulations, the average delay, average number of hops parameters, average routing traffic sent, average routing traffic received, total traffic load, average number of salvaged packets, average number of route request (RREQ) packets, average number of route reply (RREP) packets, average time for path discovery, and average number of retransmissions are used for analysing how the proposed algorithm can affect network behaviour. The final values in graphs and tables are average values collected from 100 simulation runs. Figure 10 shows simulation scenario for 20 mobile nodes in OPNET modeler.

The *average delay* provides the average amount of the time that is necessary for useful transmission of the packet between source and destination nodes. The *average number of hops represents* a number of transmissions necessary to find the end-to-end connection between a source and destination mobile node. The *average amounts of routing traffic sent and received* provide information about how many pieces of data the routing protocol needs to send to the network until the communication paths are found. The *total traffic load* indicates how the network will be loaded with the routing traffic if mobile nodes start sending data packet. Parameters *average amounts of route request (RREQ) and reply (RREP) packets* show the number of routing packets sent by routing protocol DSR to neighbors mobile nodes during a process of establishment of the communication paths. *Time for path discovery* is the average time necessary for path selection.

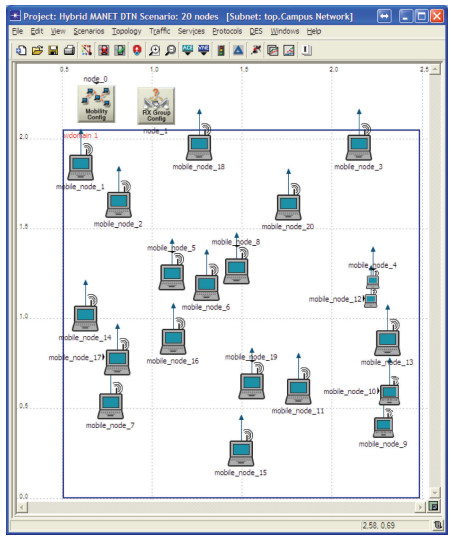



Figure 10: Example of the simulation scenario with randomly placed mobile nodes in OPNET modeler.

The *average amounts of the salvaged packets* give us information about how many packets were salvaged by routing protocol during routing or forwarding. The *average amounts of retransmissions* show how many times are necessary for resending the routing packet if the communication paths are disconnected. The *average amounts of the salvaged packets* give us information about how many packets were salvaged by routing protocol during routing or forwarding.

*3.1. Comparison of the MANET and DTN in Disconnected Environment.* In this section, we present the numerical results, depicting the relation between DSR (MANET) and DTN in a disconnected environment. We analyse how the disconnection of the communication paths affects the behaviour of the network. The simulations are focused on the situations when communication paths are disconnected for a short time interval while routing protocol cannot establish an end-to-end connection. The results also show why MANET cannot be used for delivering of the messages in this environment. In these simulations, we simulate the disconnection of the communication paths. The disconnection of the communication paths was simulated with short transmission ranges on nodes and by using random mobility model. The mobile nodes were moved randomly across the network with randomly selected speed and the DSR routing protocol cannot establish communication paths between mobile terminals. For this reason, an average delay and an average number of hops have been analysed. Collected results show why integration between DSR (MANET) and DTN routing mechanisms is necessary.

Figure 11 shows the average delay for DSR (MANET) and DTN models with respect to the different number and moving speed of mobile nodes. If the communication paths were disconnected, the values were higher for DSR (MANET) than for DTN. Based on the idea of DSR, the routing mechanism sends the routing packets in order to

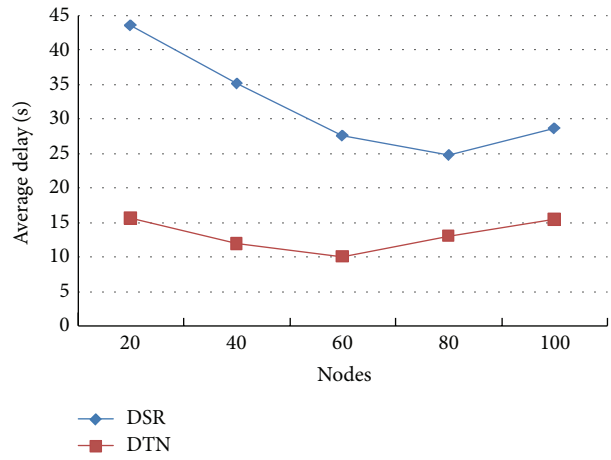



Figure 11: Average delay for DTN (MANET) and DTN in disconnected environment.

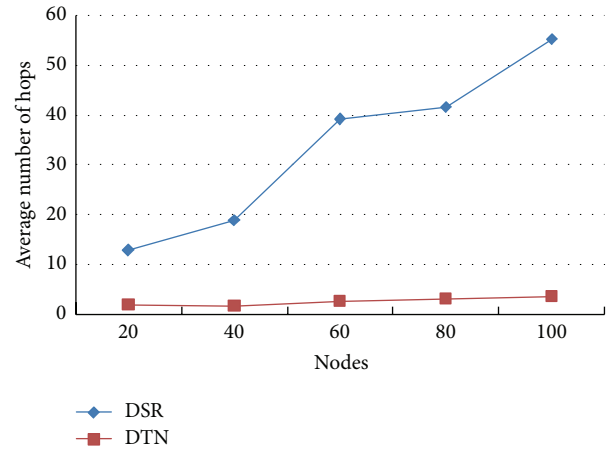



Figure 12: Average number of the hops for MANET and DTN in disconnected environment.

find communication paths and, on the other side in DTN, the PRoPHET protocol unicast only the packet for the nodes which are directly connected to the selected mobile node. We can also see that delay for 60, 80, and 100 nodes is increased for DTN. This situation is explained by the fact that the DTN forward messages directly to selected relay node or nodes that are randomly across the simulation area until they find a suitable node to transport message. The node may not be a node that is looking for the shortest path between the source and the destination node. The values of average delay for DSR (MANET) are almost 2 times higher than values for DTN.

The second analysed parameter is the average number of hops. Model DSR provides the routing mechanisms if the communication paths are disconnected that is resulting in a significant number of hops for networks with the highest number of the mobile nodes (Figure 12). In DTN, the PRoPHET protocol enables finding destination node with the lower number of hops based on the idea of the forwarding mechanism. If the communication paths are disconnected for a short time the DTN shows better results in comparison with MANET (Figures 11 and 12).

Table 2: Values of the average routing traffic send [kbit/s] for different number and speed of nodes.

| Number of nodes | Model | Speed of nodes | | |
|---|---|---|---|---|
| | | 2 m/s | 4 m/s | 6 m/s |
| 20 | DSR | 0.708 | 0.753 | 0.651 |
| | DSR_TRUST1 | 0.701 | 0.826 | 0.948 |
| | DSR_TRUST2 | 0.712 | 0.823 | 0.922 |
| 40 | DSR | 1.040 | 2.003 | 1.185 |
| | DSR_TRUST1 | 1.990 | 2.399 | 3.204 |
| | DSR_TRUST2 | 2.134 | 2.249 | 3.127 |
| 60 | DSR | 2.061 | 3.299 | 2.440 |
| | DSR_TRUST1 | 2.925 | 2.161 | 4.958 |
| | DSR_TRUST2 | 2.743 | 2.082 | 4.422 |
| 80 | DSR | 4.090 | 5.931 | 3.911 |
| | DSR_TRUST1 | 5.983 | 6.562 | 7.626 |
| | DSR_TRUST2 | 5.878 | 6.336 | 7.448 |
| 100 | DSR | 8.306 | 8.784 | 10.001 |
| | DSR_TRUST1 | 9.122 | 11.395 | 12.695 |
| | DSR_TRUST2 | 8.767 | 10.826 | 11.947 |

Table 3: Values of the average routing traffic received [kbit/s] for different number and speed of nodes.

| Number of nodes | Model | Speed of nodes | | |
|---|---|---|---|---|
| | | 2 m/s | 4 m/s | 6 m/s |
| 20 | DSR | 1.098 | 1.568 | 1.663 |
| | DSR_TRUST1 | 1.306 | 4.136 | 1.584 |
| | DSR_TRUST2 | 1.300 | 4.001 | 1.509 |
| 40 | DSR | 2.067 | 3.086 | 2.,185 |
| | DSR_TRUST1 | 6.847 | 2.851 | 2.478 |
| | DSR_TRUST2 | 6.732 | 2.586 | 2.317 |
| 60 | DSR | 4.999 | 7.243 | 6.594 |
| | DSR_TRUST1 | 12.019 | 8.843 | 9.482 |
| | DSR_TRUST2 | 11.362 | 8.556 | 9.212 |
| 80 | DSR | 8.317 | 10.056 | 7.897 |
| | DSR_TRUST1 | 14.497 | 13.421 | 12.329 |
| | DSR_TRUST2 | 14.019 | 13.114 | 12.098 |
| 100 | DSR | 16.015 | 16.237 | 16.104 |
| | DSR_TRUST1 | 28.094 | 23.026 | 32.103 |
| | DSR_TRUST2 | 27.551 | 22.888 | 31.922 |

*3.2. Network Analysis of the Hybrid MANET-DTN in Disconnected Environment.* In these simulations, we analyse the network performance analysis of three models DSR, DSR_TRUST1, and DSR_TRUST2 from the routing perspective. The main idea is to study how the implementation of algorithms can affect the routing mechanisms and also how the implementation of the designed mechanisms can affect the total network performance. This simulation is focused on the situation when the communication paths will be disconnected during transmission of the data. In this case, the routing paths will be broken and trust algorithm will be activated in order to find the relay node. This selected trusted relay node then will transport messages until the connection to another node is established.

During simulation, the average amount of routing traffic sent, an average amount of routing traffic received, total traffic load, an average number of route request (RREQ) packets, an average number of route reply (RREP) packets, an average number of retransmissions, and an average time for path discovery are analysed. Parameters give us an analysis of how the implementation of the proposed algorithms will affect the routing processes for different speed and the number of the mobile nodes.

Tables 2 and 3 show how the average routing data sent and received is impacted by the disconnection of the communication paths. In the case of disconnected communication paths, the results increase with higher speed and number of the mobile nodes. Model DSR_TRUST1 has generally the highest average routing traffic sent and received as compared to DSR. We obtained better results for model DSR_TRUST2 due to the existence of an enhanced trust algorithm, which is implemented directly in the mobile nodes. The routing data are resent only if the mobile node is trusted. Enhancement also enables using the contact history, which gives better possibilities of finding a trusted relay node for transportation of the data in the situation when the communication paths are disconnected.

Table 4: Values of the total traffic load [kbit/s] for different number and speed of nodes.

| Number of nodes | Model | Speed of nodes | | |
|---|---|---|---|---|
| | | 2 m/s | 4 m/s | 6 m/s |
| 2 | DSR | 4.571 | 4.164 | 4.496 |
| | DSR_TRUST1 | 2.841 | 3.509 | 3.656 |
| | DSR_TRUST2 | 1.300 | 2.851 | 3.296 |
| 40 | DSR | 9.983 | 13.964 | 11.057 |
| | DSR_TRUST1 | 8.336 | 7.976 | 12.133 |
| | DSR_TRUST2 | 5.739 | 6.663 | 9.583 |
| 60 | DSR | 16.752 | 20.712 | 14.713 |
| | DSR_TRUST1 | 15.540 | 18.323 | 14.474 |
| | DSR_TRUST2 | 10.546 | 15.410 | 13.569 |
| 80 | DSR | 29.121 | 31.472 | 23.964 |
| | DSR_TRUST1 | 21.255 | 25.244 | 23.332 |
| | DSR_TRUST2 | 17.902 | 21.202 | 22.045 |
| 100 | DSR | 44.789 | 44.074 | 45.658 |
| | DSR_TRUST1 | 44.224 | 40.231 | 34.456 |
| | DSR_TRUST2 | 39.164 | 37.457 | 40.127 |

Table 4 shows the network performance analysis of these models in terms of the total traffic load for the situation that communication paths are disconnected. In this situation, the DSR routing protocol limited transport to only the routing packets in order to find communication paths. As can be viewed, the network performance of the DSR_TRUST2 is better in all situations and for networks with the lower number

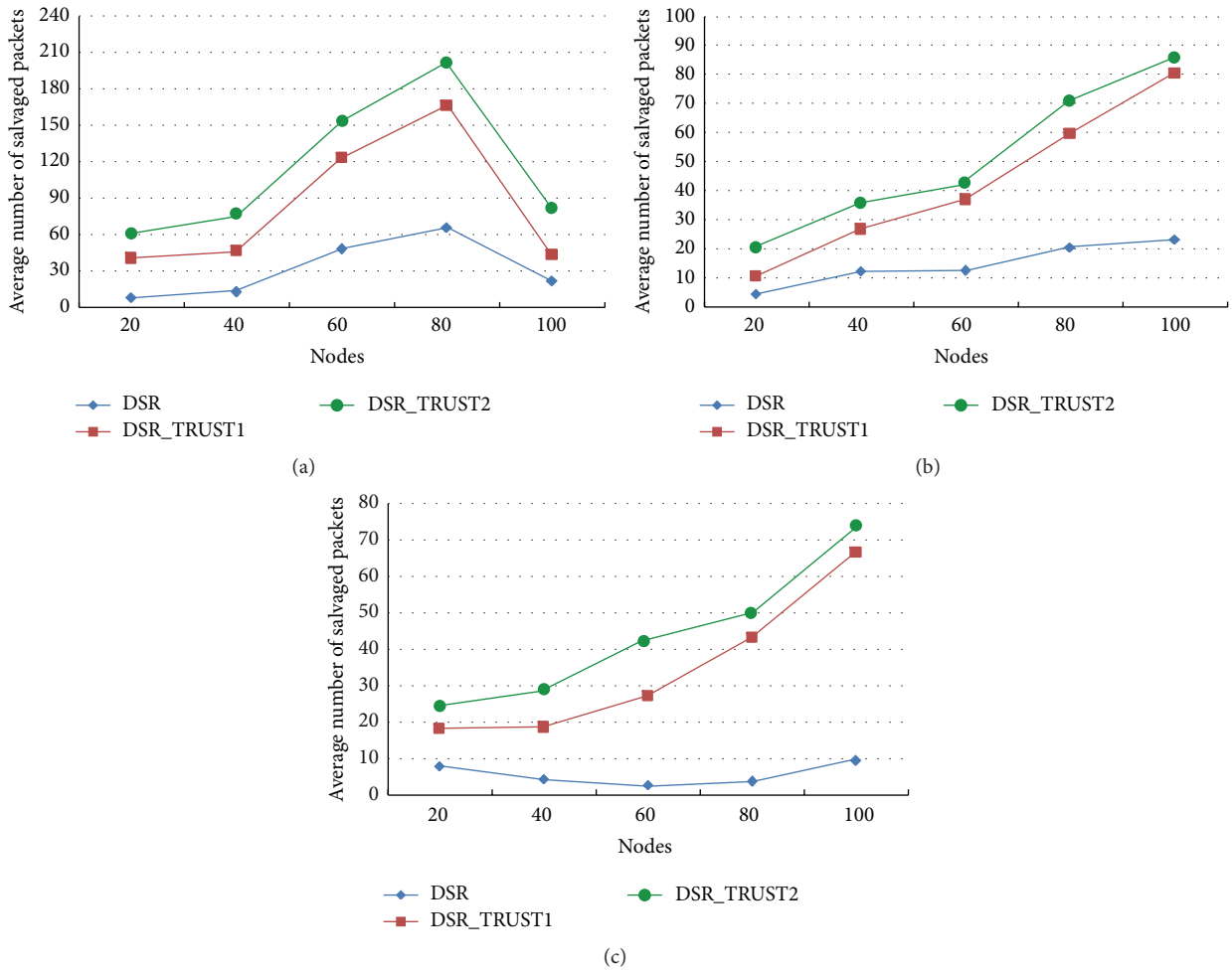



Figure 13: Average number of salvaged packets for different speed of mobile nodes: (a) 2 m/s, (b) 4 m/s, and (c) 6 m/s.

of mobile nodes. The models (DSR_TRUST1, DSR_TRUST2) obtain better results in comparison with DSR, but these models enable transportation routing and data packet via a trusted relay node in the situation when communication paths are disconnected or if there are no available mobile nodes for communication. In this situation, the PRoPHET forwarding mechanism has been activated.

Tables 5 and 6 summarize the average number of RREQ and RREP packets sent to the network while communication paths are discovered and established. Results show that model DSR_TRUST2 provides better results in all cases. If the communication paths will be disconnected, model DSR resends a lot of routing packets and in this way the network will be loaded only by routing packets. On the other side, model DSR_TRUST1 enables selecting relay node only based on the routing parameters (see Section 2.1) and relay node selection will be impacted in a negative sense by this situation. The proposed extension (DSR_TRUST2) eliminates this situation and it enables selecting trusted relay node with respect to contact history. It also provides the ability to decrease the number of routing packets sent to the network. It means that DSR_TRUST2 enables decreasing the number of sent RREQ packets on the network and also

Table 5: Average number of route request (RREQ) packets [packets/s] for different number and speed of nodes in hybrid MANET-DTN.

| Number of nodes | Model | Speed of nodes | | |
|---|---|---|---|---|
| | | 2 m/s | 4 m/s | 6 m/s |
| 20 | DSR | 324.340 | 489.390 | 675.30 |
| | DSR_TRUST1 | 302.661 | 405.692 | 456.610 |
| | DSR_TRUST2 | 167.851 | 348.543 | 368.324 |
| 40 | DSR | 336.771 | 542.561 | 583.357 |
| | DSR_TRUST1 | 183.331 | 390.809 | 402.985 |
| | DSR_TRUST2 | 173.856 | 348.539 | 368.324 |
| 60 | DSR | 592.317 | 734.418 | 794.139 |
| | DSR_TRUST1 | 542.321 | 663.294 | 683.647 |
| | DSR_TRUST2 | 502.534 | 612.300 | 633.614 |
| 80 | DSR | 836.000 | 1236.567 | 1297.153 |
| | DSR_TRUST1 | 765.431 | 889.441 | 1000.823 |
| | DSR_TRUST2 | 675.429 | 702.324 | 921.229 |
| 100 | DSR | 914.437 | 1174.587 | 1232.418 |
| | DSR_TRUST1 | 803.428 | 923.538 | 1103.294 |
| | DSR_TRUST2 | 751.780 | 837.411 | 963.610 |

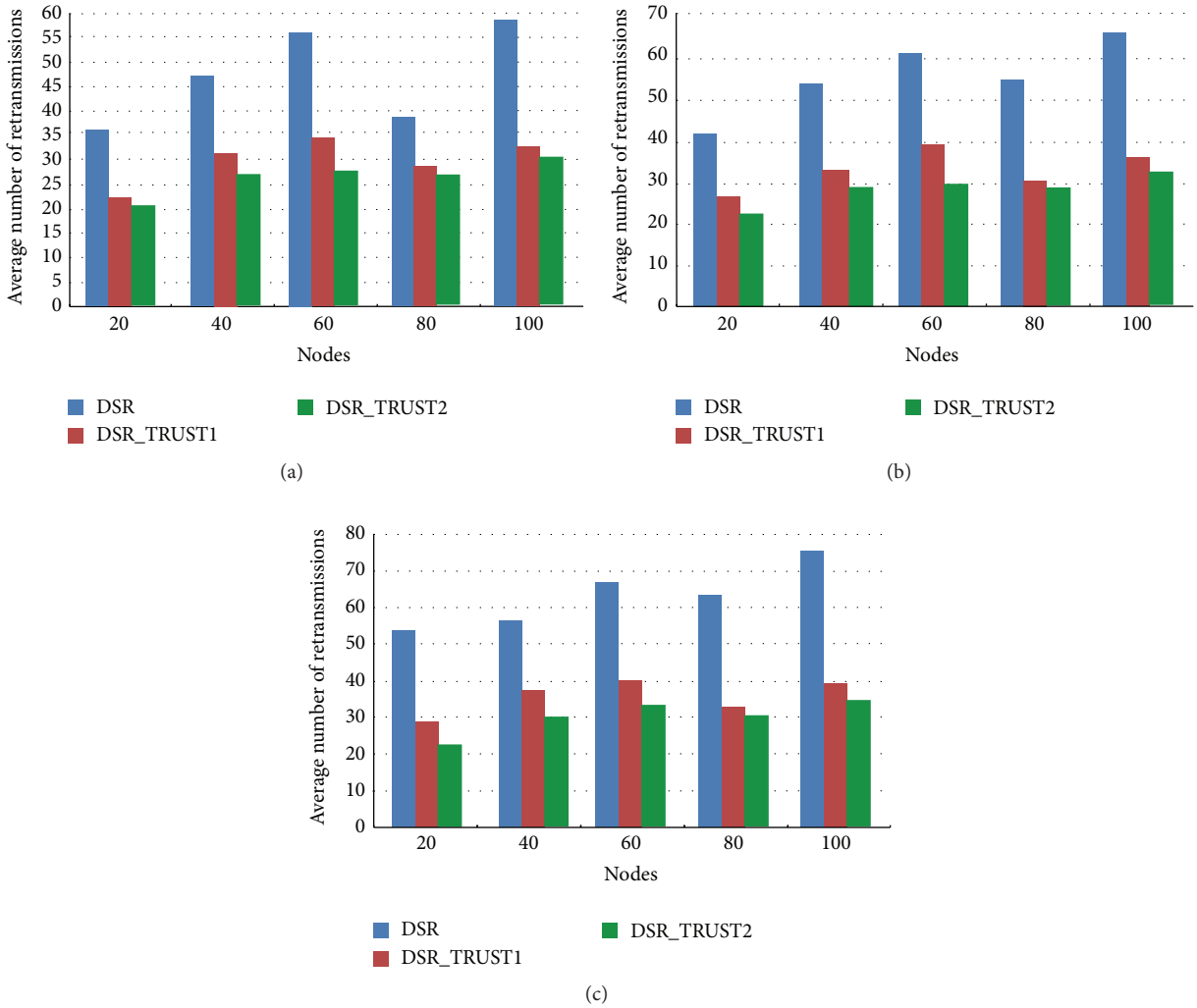



Figure 14: Comparison of the average number of retransmissions for different speed of mobile nodes: (a) 2 m/s, (b) 4 m/s, and (c) 6 m/s in disconnected environment.

enables increasing the average number of RREP used for the establishment of the communication paths. These results are in a strong correlation with results from Section 3.1.

The average number of salvaged packets is discussed too. Figure 13 shows how many packets are salvaged during the sending of routing packets in disconnected environments. The graphical result shows that implementation of models DSR_TRUST1 and DSR_TRUST2 to secure the selection of relay node enables salvaging a lot of packets in comparison with DSR model. It stems from the fact that the algorithms allow selecting only trusted nodes for transmission of messages between the mobile environments. We can see, from the results, that implementation of the DSR_TRUST1 and DSR_TRUST2 provides higher values of the salvage packets in all situations. On the other side, if the speed of mobile nodes is increased, the number of salvaged packets begins to dramatically fall down for model DSR in comparison with models DSR_TRUST1 and DSR_TRUST2. We can conclude that the selection of the relay nodes gives the opportunities to transport messages between mobile nodes and save more packets from dropping. The proposed algorithms allow saving a lot of packets for networks with the lower number of mobile nodes that are moving with lower speed across the network.

Figure 14 gives information about how many retransmissions are necessary to be resent from nodes to the network while the communication path between nodes is established. Results show that models DSR_TRUST1 and DSR_TRUST2 decrease the number of retransmissions in comparison with DSR in disconnected environments. The trust algorithm for a relay node selection enables selection of the nodes that have a higher possibility of establishing the trusted routing paths between nodes in disconnected environments. We can also see that using history of contact is a simple and useful tool, implemented in DSR_TRUST2, such that it allows reducing this value to the minimum.

Next studied parameter is the average time for path discovery. The parameter gives information about time that is required for the establishment of the communication path between mobile nodes. Based on the results showed

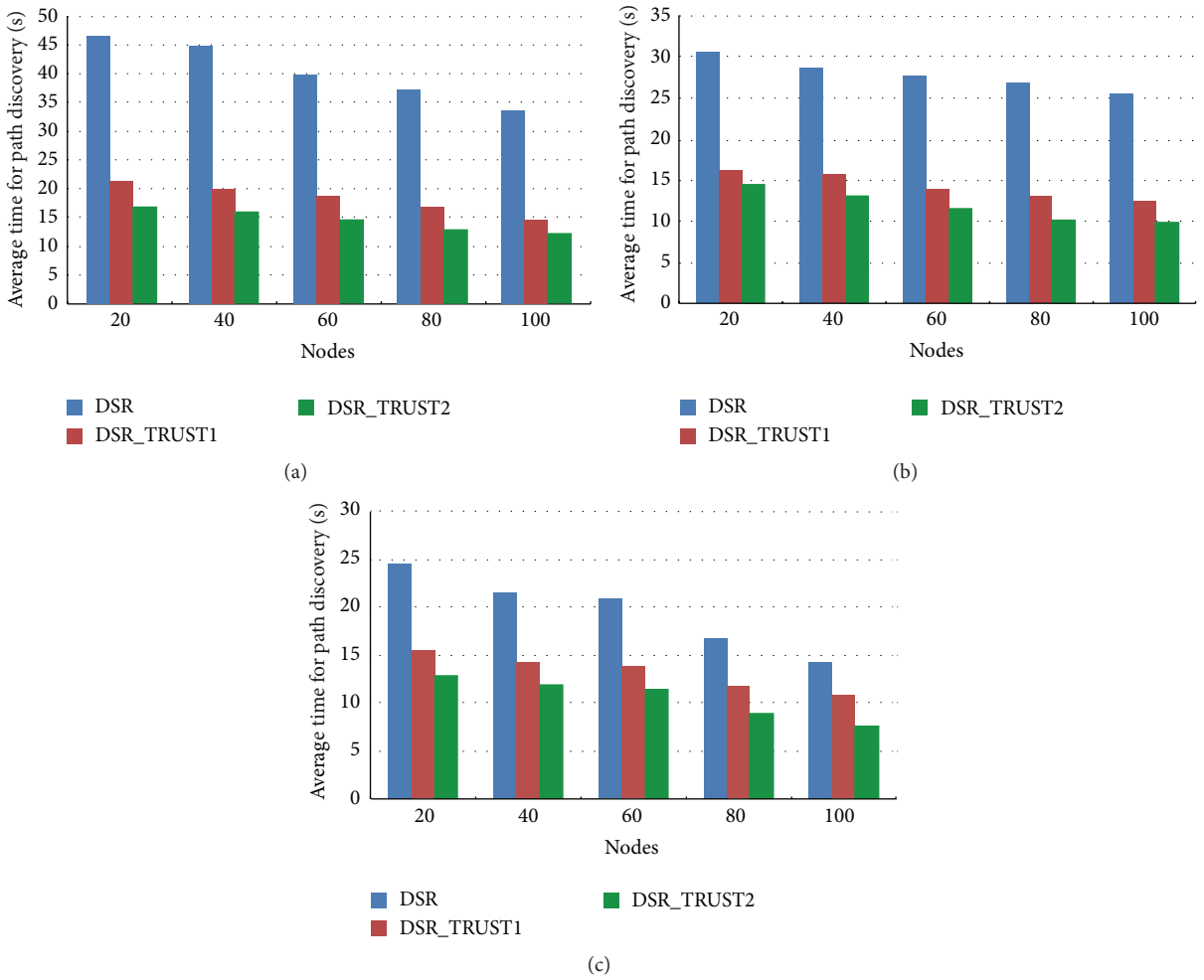



Figure 15: Comparison of the average time for path discovery for different speed of mobile nodes: (a) 2 m/s, (b) 4 m/s, and (c) 6 m/s in disconnected environment.

Table 6: Average number of route reply (RREP) packets [packets/s] for different number and speed of nodes in hybrid MANET-DTN.

| Number of nodes | Model | Speed of nodes | | |
|---|---|---|---|---|
| | | 2 m/s | 4 m/s | 6 m/s |
| 20 | DSR | 10.741 | 11.978 | 21.251 |
| | DSR_TRUST1 | 23.214 | 24.650 | 32.331 |
| | DSR_TRUST2 | 31.524 | 31.433 | 43.424 |
| 40 | DSR | 10.641 | 10.561 | 10.437 |
| | DSR_TRUST1 | 13.446 | 16.382 | 17.673 |
| | DSR_TRUST2 | 14.331 | 17.321 | 20.218 |
| 60 | DSR | 13.654 | 12.651 | 12.117 |
| | DSR_TRUST1 | 18.333 | 17.771 | 15.608 |
| | DSR_TRUST2 | 20.138 | 21.322 | 19.628 |
| 80 | DSR | 17.425 | 21.538 | 22.578 |
| | DSR_TRUST1 | 21.438 | 27.360 | 30.150 |
| | DSR_TRUST2 | 23.527 | 29.325 | 36.110 |
| 100 | DSR | 24.441 | 30.129 | 34.537 |
| | DSR_TRUST1 | 28.253 | 37.647 | 40.231 |
| | DSR_TRUST2 | 33.451 | 44.318 | 46.312 |

in Figure 15 we can conclude that model DSR_TRUST2 needs less time in comparison with model DSR_TRUST1. On the other side, model DSR requires more time to establish the communication paths. We can also see that those implemented algorithms in DSR_TRUST1 and DSR_TRUST2 models provide the possibility of finding a path if there are disconnected ones and also the possibility of shortening the time for path establishment if routing protocol DSR cannot find communication paths.

## 4. Conclusion

Hybrid MANET-DTN is an evolution of mobile networks that integrate MANET and DTN into one complex network. Hybrid MANET-DTN enables transportation of the data between different mobile terminals in the situation when the communication paths are disconnected or never exist. The communication does not rely on end-to-end connection, but it is based on the *store-carry-forward* model integrated from DTN. Hybrid MANET-DTN give new challenges for a new application and services. The main idea of hybrid MANET-DTN provides the ability to use the network not

only for personal use but also for emerging applications and services. The main problem of the hybrid MANET-DTN is security and relay node selection. In the paper, we introduce two models for the secure selection of the relay nodes based on the trust.

In the paper, the network performance analysis of the proposed algorithms is presented. The goal of the analysis demonstrates that those proposed algorithms to relay node selection do not affect the network performance. The four models DSR, DSR_TRUST1, DSR_TRUST2, and DTN have been tested in OPNET modeler. Based on collecting results we can conclude that trust algorithm for selection of the relay node provides the useful tool to a selection of the optimal trusted path in the case of disconnected environment and also this algorithm allows enhancing the performance of the hybrid MANET-DTN from the routing point of view. We show that model DSR_TRUST2 gives better results in comparison with model DSR_TRUST1. Selecting relay nodes based on contact history also enables reducing the risk of the using of the malicious mobile node.

The main problem of these algorithms is how to optimize a selection of the relay node if there is more than one node with the same values of the trust. For this reason, we will focus on the design of the method of the relay node selection based on game theory with respect to trust algorithm. The main idea of this algorithm will combine routing properties of the MANET and DTN in order to increase the performance of the hybrid MANET-DTN and also provides the secure transportation of the data across the disconnected environment.

## Competing Interests

The authors declare that they have no competing interests.

## Acknowledgments

This work has been performed in the framework of the Ministry of Education of Slovak Republic under research VEGA 1/0075/15 (100%).

## References

[1] A. Cizmar, L. Dobos, and J. Papaj, "Security and QoS integration model for MANETs," *Computing and Informatics*, vol. 31, no. 5, pp. 1025–1044, 2012.

[2] J. Papaj, L. Dobos, and A. Čižmár, "Routing strategies in opportunistic networks," *Journal of Electrical and Electronics Engineering*, vol. 5, no. 1, pp. 167–172, 2012.

[3] J. Machaj and P. Brida, "Impact of radio map simulation on positioning in indoor environtment using finger printing algorithms," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 15, pp. 6404–6409, 2015.

[4] J. Papaj and L. Dobos, "Trust based algorithm for candidate node selection in hybrid MANET-DTN," *Advances in Electrical and Electronic Engineering*, vol. 12, no. 4, pp. 271–278, 2014.

[5] M. Caleffi and L. Paura, "Opportunistic routing for disruption tolerant networks," in *Proceedings of the IEEE 23rd International Conference on Advanced Information Networking and Applications Workshops (WAINA '09)*, pp. 826–831, Bradford, UK, May 2009.

[6] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 607–640, 2012.

[7] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervelló-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 1166–1182, 2012.

[8] R. Sheikh, M. Singh Chande, and D. K. Mishra, "Security issues in MANET: a review," in *Proceedings of the Seventh International Conference on Wireless and Optical Communications Networks (WOCN '10)*, pp. 1–4, Colombo, Sri Lanka, September 2010.

[9] W. D. Ivancic, "Security analysis of DTN architecture and bundle protocol specification for space-based networks," in *Proceedings of the IEEE Aerospace Conference*, pp. 1–12, IEEE, Big Sky, Mont, USA, March 2010.

[10] Y. Li, W. Chen, and Z.-L. Zhang, "Optimal forwarder list selection in opportunistic routing," in *Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS '09)*, pp. 670–675, Macau, China, October 2009.

[11] J. P. Kurth, A. Zubov, and J. P. Redlich, "Cooperative opportunistic routing using transmit diversity in wireless mesh networks," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08)*, pp. 1310–1318, Phoenix, Ariz, USA, April 2008.

[12] M. Lu, F. Li, and J. Wu, "Efficient opportunistic routing in utility-based ad hoc networks," *IEEE Transactions on Reliability*, vol. 58, no. 3, pp. 485–495, 2009.

[13] H. Dubois-Ferriere, M. Grossglauser, and M. Vetterli, "Least-cost opportunistic routing," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*, pp. 994–1001, September 2007.

[14] P. B. Velloso, R. P. Laufer, D. D. O. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172–185, 2010.

[15] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[16] K. Ahmadi, *Decision making using trust and risk in self-adaptive agent organization [M.S. thesis]*, Utah State University, 2014.

[17] M. Li, Y. Xiang, B. Zhang, and Z. Huang, "A sentiment delivering estimate scheme based on trust chain in mobile social network," *Mobile Information Systems*, vol. 2015, Article ID 745095, 20 pages, 2015.

[18] 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, no. 5, pp. 1200–1210, 2014.

[19] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social trust in opportunistic networks," in *IEEE Conference on Computer Communications Workshops (INFOCOM '10)*, pp. 1–6, San Diego, Calif, USA, March 2010.

[20] OPNET Modeler Simulation Software, http://www.opnet.com.

[21] A. Lindgren, A. Doria, E. Davies, and S. Grasic, *Probabilistic Routing Protocol for Intermittently Connected Networks*, 2012, http://tools.ietf.org/html/rfc6693.

[22] K. Scott and S. Burleigh, *Bundle Protocol Specification*, 2007, http://tools.ietf.org/html/rfc5050.