Trust Based Algorithm for Candidate Node Selection in Hybrid MANET-DTN

Jan PAPAJ, Lubomir DOBOS

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

jan.papaj@tuke.sk, lubomir.dobos@tuke.sk

Abstract. *The hybrid MANET-DTN is a mobile network that enables transport of the data between groups of the disconnected mobile nodes. The network provides benefits of the Mobile Ad-Hoc Networks (MANET) and Delay Tolerant Network (DTN). The main problem of the MANET occurs if the communication path is broken or disconnected for some short time period. On the other side, DTN allows sending data in the disconnected environment with respect to higher tolerance to delay. Hybrid MANET-DTN provides optimal solution for emergency situation in order to transport information. Moreover, the security is the critical factor because the data are transported by mobile devices. In this paper, we investigate the issue of secure candidate node selection for transportation of the data in a disconnected environment for hybrid MANET-DTN. To achieve the secure selection of the reliable mobile nodes, the trust algorithm is introduced. The algorithm enables select reliable nodes based on collecting routing information. This algorithm is implemented to the simulator OPNET modeler.*

Keywords

Candidate node, delay tolerant network, mobile ad-hoc network, trust.

1. Introduction

Mobile ad-hoc network (MANET) is characterized by multi hop communication between mobile nodes by wireless links [1]. There are also no infrastructures and routing paths established by routing algorithms (Fig. 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. Data packets are then transmitted from one intermediate relay node to the next specified relay based on physical condition of wireless channels [2], [4], [5]. The routing algorithm relies on the assumption that the network graph is fully connected and fails to route messages if there is not a complete route from source to destination at the time of sending [3].

The Delay/Disruption Tolerant Networks (DTN) or Opportunistic networks (OppNet) 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 or OppNet can be deployed in environment, where high bit error rates and the long-term disconnections are experienced. These are proposed and designed to operate in hostile environments. The one is characterized by very long delay paths and frequent network partitions [6].

Security is an important issue in MANET, DTN and OppNet. In MANET, the security mechanisms are

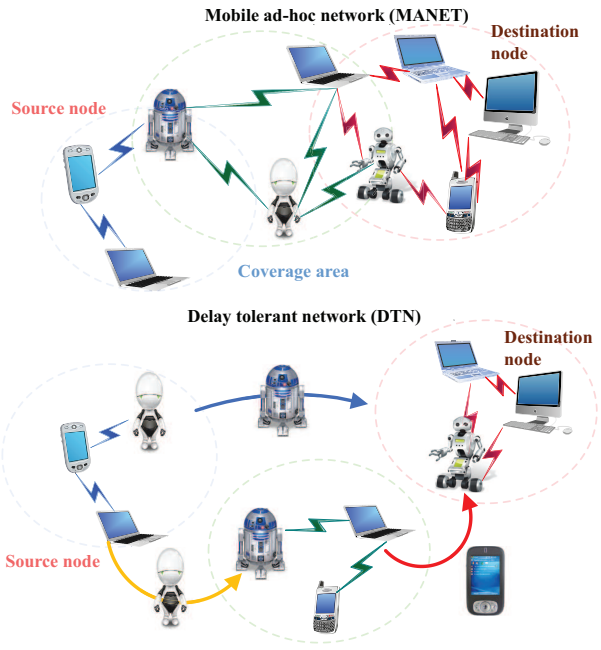


Fig. 1: Difference between MANET and DTN.

based on the assumption that there is/are a connection between source and target nodes (end-to-end connections) [2]. In OppNet, we require the security solutions, which provide security for all nodes, all services and application that participate in routing and transmitting process. There is a sporadic connectivity of nodes and we need to provide secure delivery of the messages from source node to the destination node.

In order to provide the effective communication between nodes, there is necessary to consider different aspects (disconnections, mobility, partitions, and norms instead of the exceptions). The mobility in opponent is used to provide efficient communication between unconnected groups of nodes. 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 candidate node is the first key issue. There are a few works which deal with the selection of the candidate nodes. The firs 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 [6]. Other algorithms are based on link state algorithm for the unconstrained selection based on the Dijkstra algorithm [7]. Most methods are based on generalizing the Bellman-Ford algorithm and they prove its optimality [8], [9].

In this article the trust based candidate node selection algorithm is introduced. This mechanism enables the selection of the secure mobile node used for transportation of the data across the disconnected environment. Selected candidate nodes provide the secure mobile node selected to transport of the data. If the mobile node finds connection the DTN forwarding mechanism is activated.

1.1. Trust Mechanisms for Hybrid MANET-DTN

The term of trust is defined in different disciplines. Trust enables to combine many different aspects and then can be reflected by reliability, utilization, availability, reputation, risk, confidence, quality of services and other concepts. Trust enables to calculate a subjective assessment by a mobile node based on reliability and accuracy of information received from or traversing through that node in a given context.

In hybrid MANET-DTN, the key aspect is how these trust concepts can be applied in modeling trust [10], [11]. Trust calculation can be divided into the following groups (Fig. 2):

- Direct trust calculation - mobile nodes have implemented mechanisms for computing its own value of the trust on its neighbours.
- Indirect trust calculation - the trust is computed based on the recommendation of the neighbour mobile nodes.
- Hybrid trust calculation - combination of the direct and indirect method.

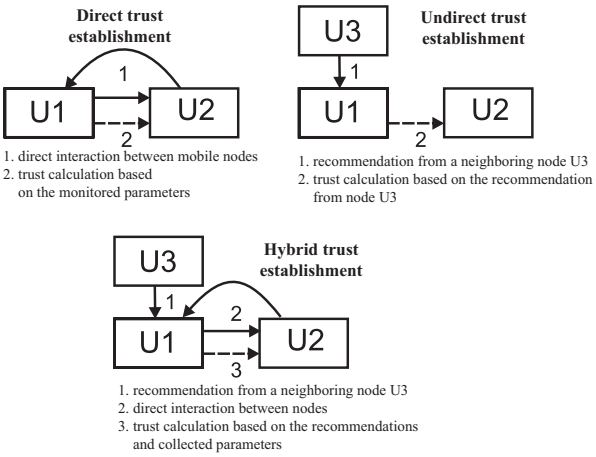


Fig. 2: Trust computation models for hybrid MANET-DTN.

2. Proposed Trust Algorithm for Hybrid MANET-DTN

The proposed algorithm is based on the direct model for the trust computation. This model is based on the assumption that each node in the network receives information about other nodes. Information is stored on each node and later used in the calculation of the resulting values of trust. The algorithm is designed on third layer so that all obtains from the node information throughout the entire operation of the network layer.

The data and routing streams are monitored. Figure 3 shows the flow diagram of the proposed algorithm for calculation of trust. The algorithm can be divided into two main phases:

- Phase of obtaining and storing information.
- Phase of trust computing.

These phases are carried out whenever the packet is received on the node. It is for this reason that the final value of 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.

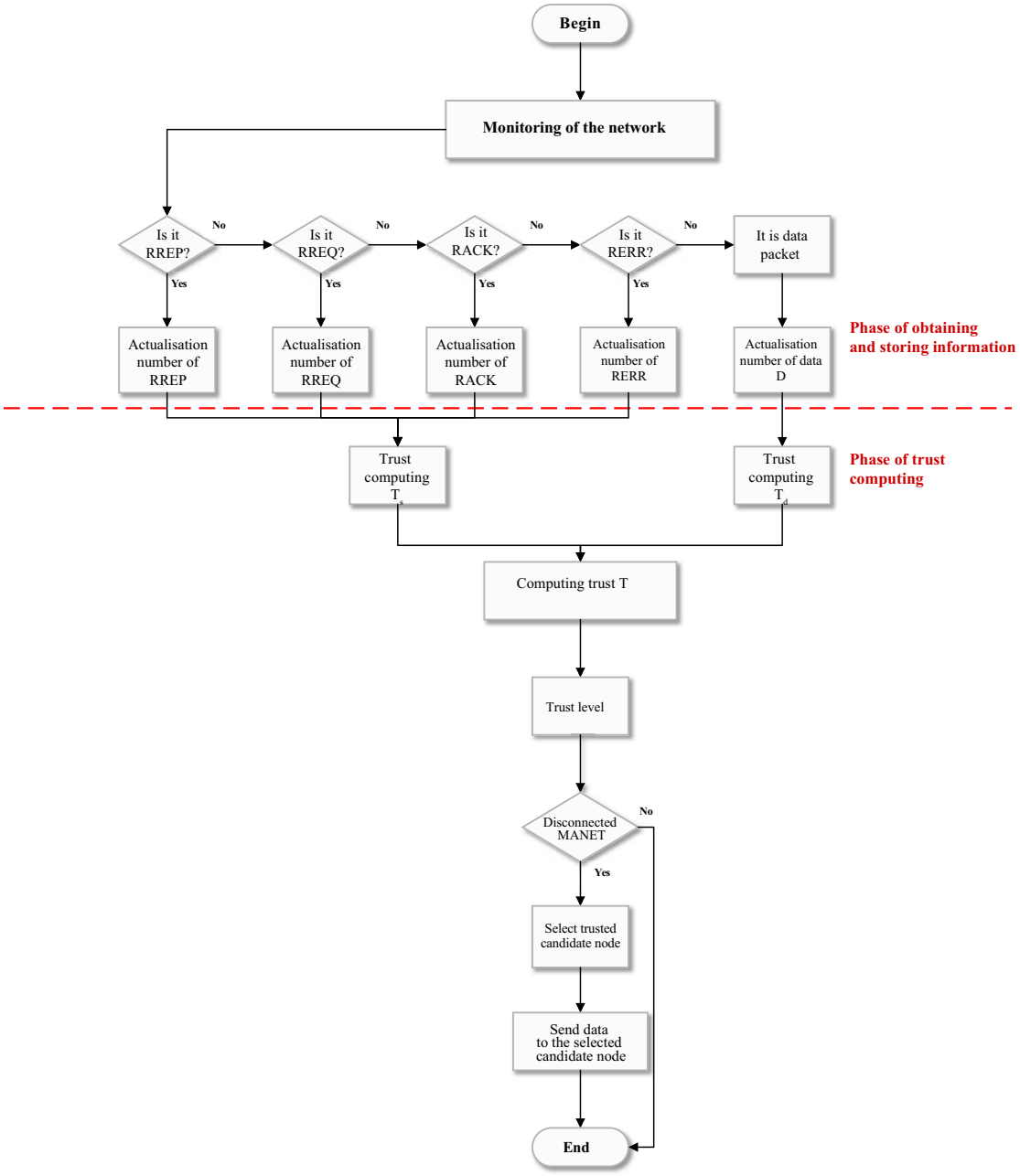


Fig. 3: Proposed algorithm for trust monitoring in hybrid MANET-DTN.

2.1. 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.

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

number of route errors received from each node, number of route reply received from each node, number of data packets received from each node.

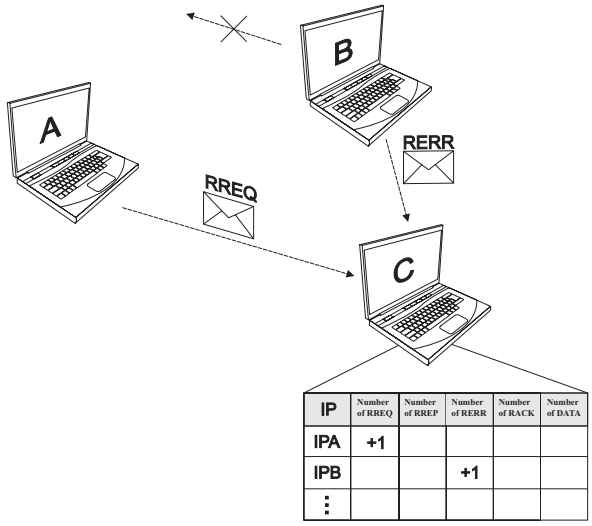


Fig. 4: Collecting of the routing data from hybrid MANET-DTN.

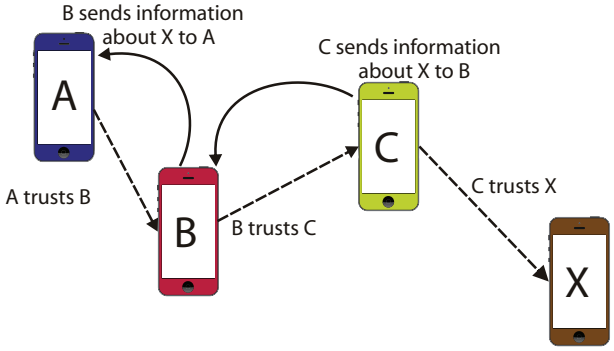


Fig. 5: Promotion calculated value confidentiality between nodes during computing of the trust in hybrid MANET-DTN.

This information from the phase of obtaining and saving of parameters are stored in the data structure in memory on each node separately. Each node contains information about nodes with whom he came in contact, and when they exchange routing information or data traffic between each other. Each node in the network is separate and calculates a resulting value of confidentiality to the other node. Information is stored in a format which has the form of a table. This structure is dynamic and its size can vary based on the number of nodes with which node communicates.

Figure 4 illustrates the phase of obtaining and saving parameters. In the picture we can see three communicating nodes A, B, C. In this scenario, node A sends a packet type Route Request to node C and node B sends a Route error packet to the node C (Fig. 4). From node C point of view, this node updates the parameter table and store 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.

2.2. Phase of Computing Trust Parameter

After retrieving and updating the parameters in table of parameters for each node, it is necessary to calculate and update the value of trust. At this stage, the value of 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. Serves locally on that node and helps him in deciding. In our case, the calculated value will serve by the decision on sending in a situation where there is a disconnection in the network and the node will not have a backup path to the destination node (Fig. 5). The actual calculation of confidentiality can be divided into two parts:

- Trust calculation from routing information.
- Trust calculation from data packets.

From these two sub-calculations we get the final value of trust, which is registered in the node data structure. Analyze individual fragment values are given in equations:

$$T_s = W_{rreq} \cdot \left(\frac{R_{req}}{R_{reqc}}\right) + W_{rrep} \cdot \left(\frac{R_{rep}}{R_{repc}}\right) + \\ + W_{rerr} \cdot \left(\frac{R_{rerr}}{R_{rerrc}}\right) + W_{rack} \cdot \left(\frac{R_{rack}}{R_{rackc}}\right), \quad (1)$$

$$T_d = W_d \cdot \left(\frac{D}{D_c}\right), \quad (2)$$

where T_s and T_d are mentioned partial value confidentiality. Furthermore W_{rreq}, W_{rrep}, W_{rerr}, W_{rack}, 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 each type of packets from specific nodes in the network. Values R_{rreqc}, R_{rrepc}, R_{rerrc}, R_{rackc}, D_c represent the total number of packets received on the node from all nodes and R_{rreq}, R_{rrep}, R_{rerr}, R_{rack}, D are the values of packets received from each nodes. The value representing final trust is shown in Eq. (3):

$$T = T_s + T_d, \quad (3)$$

where T is the resulting value of confidentiality and T_s and T_d values is partial confidentiality mentioned above.

3. Simulations and Results

OPNET modeler simulator a professional tool was used for testing of the proposed mechanisms. OPNET provides a lot of useful tools for analyzing of the mobile networks and enables to simulate mobile ad-hoc networks with different routing protocol [12]. The Dynamic Source Routing protocol represents a reference value for analyzing of behaviour of the MANET [1]. In order to check the functionality of the DTN network, we have implemented a PRoPHET forwarding mechanism to the simulator OPNET modeler [12].

Tab. 1: Simulation setup for OPNET modeler.

Parameters	Values
Routing protocols	DSR, DSR_TRUST, PRoPHET
Routing parameters DSR	Default
Simulation area	2000 m×2000 m
Time of simulation	600 s
Transmission range	250 m
Number of nodes	20, 40, 60, 80, 100
Speed of nodes	$0 - 6$ m·s^{-1}
Model placement	Random
Mobility model	Default Random Waypoint with pause time 10 s
Transmitted power	1 mW
Values of trust	$W_{rreq} = 0.2$, $W_{rrep} = 0.5$, $W_{rerr} = 0.2$, $W_{rack} = 0.2$, $W_d = 0.3$
Number of values per simulation	1000

The following simulation scenarios were used to analyse the performance of the proposed mechanisms:

- MANET model - MANET network used standard DSR protocol without the possibility to find communication paths between mobile nodes.
- MANET model with TRUST - MANET network used the DSR protocol with the possibility to find candidate node based on trust.
- DTN model - network implements the PRoPHET protocol and mechanism enable to find a communication path if the links are disconnected during the transportation of the packets. The PRoPHET forwarding mechanism is implemented.

The simulation parameters for the OPNET modeler are summarized in the Tab. 1. During simulations, the average delay, average number of hops parameters, average routing traffic sent, average routing traffic received and an average number of salvaged packets, are used to check the functionalities of the proposed solution.

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 numbers of routing traffic send and received inform how many data the routing protocol needs to send to the network until the communication paths will be found. The average numbers of the salvaged packets give us information how many packets were salvaged by routing protocol while routing or forwarding. Average number of hops represents number of transmissions necessary to find end-to-end connection between source and destination mobile node. During the analysis, the average values of the parameters were analyzed.

3.1. Comparison of the MANET and DTN

This experiment is focused on the situation when all communication paths are disconnected for a short time interval. The two routing protocols for MANET and DTN namely DSR and PRoPHET were analyzed. The disconnection of the communication paths was simulated with short transmission ranges and random mobility model. This mobility model enables to move mobile node across the simulation area randomly with randomly selected speed. Disconnections represent a short time interval when DSR routing protocol for MANET cannot find a communication path with other mobile nodes. Parameters average delay and average number of hops were analyzed. Collected results show why integration between MANET and DTN routing mechanisms are necessary.

Figure 6 shows the average delay for MANET and DTN with respect to the number of the mobile nodes with different speed. If the communication paths were disconnected, the values are higher for MANET than PRoPHET. Based on the idea of DSR, the routing mechanism sends the routing packets in order to find communication paths and on the other side PRoPHET protocol unicast only the packet for the nodes which are

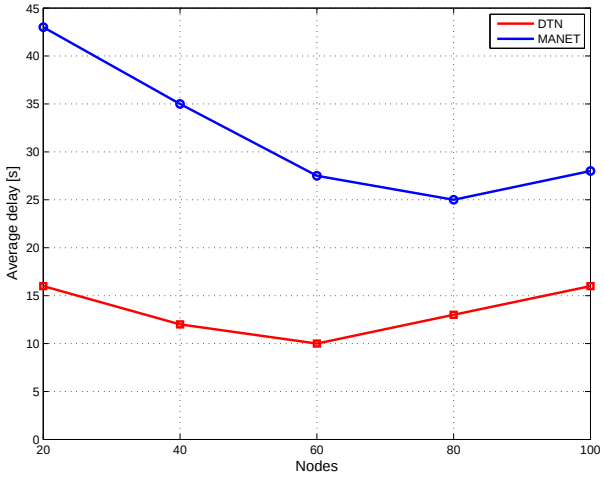


Fig. 6: The average delay for MANET and DTN.

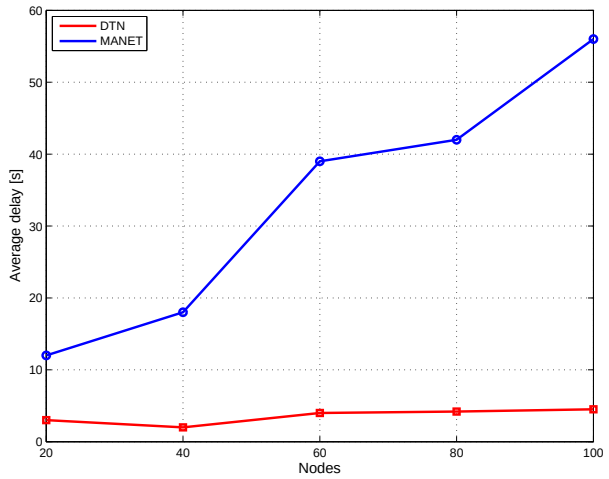


Fig. 7: The average number of the hops for MANET and DTN.

directly connected to the selected mobile node. The values of average delay for MANET are almost 2 times higher than values for DTN.

The second analyzed parameter is the average number of hops. The DSR protocol provides the routing mechanism if the communication paths are disconnected which is resulting in a significant number of the hops for networks with the highest number of the mobile nodes (Fig. 7). The PRoPHET protocol enables to find destination node with lower number of the hops based on the idea of the forwarding mechanism. If the communication paths are disconnected for a short time the PRoPHET shows the better performance than DSR routing protocol for MANET (Fig. 6, Fig. 7).

3.2. Analysis of the Routing Parameters in Disconnected Environment

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 best candidate node with regards to trust.

During simulation, the average amount of routing traffic sent, average amount of routing traffic received, an average number of dropped packets are analyzed. Parameters give us information how the new algorithm will affect the routing of the data with regard to different speed of the mobile nodes.

Table 2 and Tab. 3 show impact of the speed of the mobile nodes on average routing data sent and received. In the case of disconnected communication paths, the results increase with a higher speed and number of the mobile nodes. DSR with trust has generally the highest average routing traffic sent and received as compared to DSR routing protocol without the trust mechanism. The reason for this behaviour is the existence of trust mechanism on the mobile nodes and for this reason the routing data are resend if the mobile node is untrusted.

Tab. 2: Average routing traffic sent vs number of mobile nodes [bit·s^{-1}].

Number of nodes	Model	Speed of mobile nodes		
		2 m·s^{-1}	**4 m·s^{-1}**	**6 m·s^{-1}**
20 nodes	DSR	708.15	752.55	650.50
	TRUST	700.70	826.34	947.68
40 nodes	DSR	1039.50	2003.12	1185.29
	TRUST	1989.60	2399.20	3204.34
60 nodes	DSR	2061.00	3298.55	2439.56
	TRUST	2924.66	2160.67	4957.57
80 nodes	DSR	4090.00	5931.42	3910.58
	TRUST	5982.50	6561.55	7625.53
100 nodes	DSR	8306.24	8784.08	10000.84
	TRUST	9122.49	11394.86	12694.57

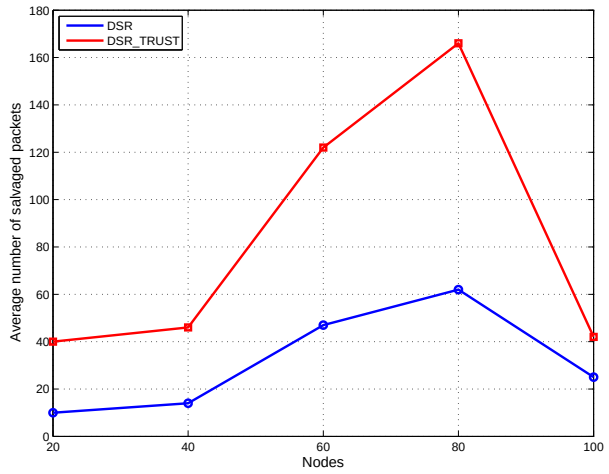
Tab. 3: Average routing traffic received vs number of mobile nodes [bit·s^{-1}].

Number of nodes	Model	Speed of mobile nodes		
		2 m·s^{-1}	**4 m·s^{-1}**	**6 m·s^{-1}**
20 nodes	DSR	1097.7	1567.5	1663
	TRUST	1306	4135.8	1583.6
40 nodes	DSR	2067	3086	2185
	TRUST	6847	2851.2	9478
60 nodes	DSR	4999	7243	6594
	TRUST	12019	8843.5	9481.5
80 nodes	DSR	8316.5	10056	7897
	TRUST	14496.5	13421	12329
100 nodes	DSR	16014	16237	16104
	TRUST	28094	23258	32103

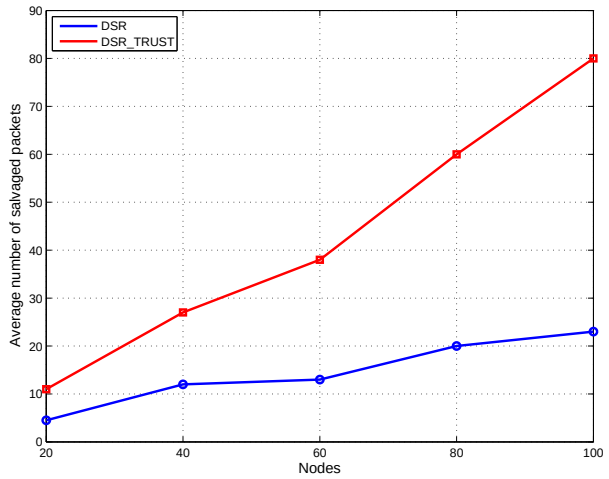
The average number of salvaged packets is another very important criterion. The one shows how many packets are salvaged during the sending of the routing packets in disconnected environments. These packets could be resend to the destination nodes. In Fig. 8, we compare the number of salvaged packets for MANET and MANET with implementing trust mechanisms versus speed of mobile nodes. Result shows, that trust algorithm to selection of candidate node enables salvage a lot of packets in comparison with DSR protocol.

4. Conclusion

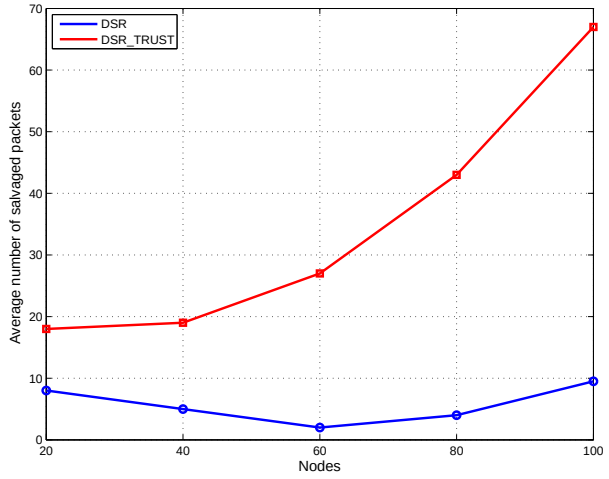
In this article, we proposed the trust algorithm for selection of the best candidate node in the hybrid MANET-DTN. The trust algorithm allows select secure mobile node for transportation of the data in a disconnected environment. The one also works in a decentralized manner. Hybrid MANET-DTN networks provides the new way how the different application could be provided for end users. The main idea of hybrid MANET-DTN networks enables use the network not



(a) 2 m·s^{-1}



(b) 4 m·s^{-1}



(c) 6 m·s^{-1}

Fig. 8: Average number of salvaged packets for different speed of mobile nodes.

only for personal usage but for emerging applications and services.

This article also gives us the basic performance analysis of the hybrid MANET-DTN networks. The models for MANET and DTN networks are implemented in OPNET modeler. Based on collecting results we can conclude trust algorithm for selection of the candidate node provides useful tool for selection of the optimal trusted path in the case of disconnected environment and also this algorithm allows enhance the performance of the hybrid MANET-DTN network from the routing point of view.

In the future we will focus on the design of the method of the candidate node selection based on game theory with regard to trust algorithm. The main idea of this algorithm is to combine routing properties of the MANET and DTN in order to increase the performance of the hybrid MANET-DTN network and also provides the secure transportation of the data across the disconnected environment.

Acknowledgment

This work has been performed partially in the framework of the Ministry of Education of Slovak Republic under research VEGA 1/0386/12 (20 %) and under research project ITMS-26220220155 supported by the Research & Development Operational Programme funded by the ERDF (80 %).

References

[1] CIZMAR, A., L. DOBOS and J. PAPAJ. Security and QoS Integration Model for MANETs. *Computing and Informatics*. 2012, vol. 31, no. 5, pp. 1025–1044. ISSN 1335-9150.

[2] PAPAJ, J., L. DOBOS and A. CIZMAR. Routing Strategies in Opportunistic Networks. *Journal of Electrical and Electronics Engineering*. 2012, vol. 5, no. 1, pp. 167–172. ISSN 1844-6035.

[3] CALEFFI, M. and L. PAURA. Opportunistic routing for disruption tolerant networks. In: *IEEE 23rd International Conference on Advanced Information Networking and Applications, AINA '09*. Bradford: IEEE, 2009, pp. 826–831. ISBN 978-1-4244-3999-7. DOI: 10.1109/WAINA.2009.201.

[4] BRIDA, P. and J. MACHAJ. A Novel Enhanced Positioning Trilateration Algorithm Implemented for Medical Implant In-Body Localization. *International Journal of Antennas and Propagation*. 2013, vol. 2013, no. 819695, pp. 1–10. ISSN 1687-5877. DOI: 10.1155/2013/819695.

[5] AMBROZIAK, S. and R. KATULSKI. An Empirical Propagation Model for Mobile Radio

Links in Container Terminal Environment. *IEEE Transactions On Vehicular Technology*. 2013, vol. 62, no. 9, pp. 4276–4287. ISSN 0018-9545. DOI: 10.1109/TVT.2013.2266618.

[6] LI, Y., W. CHEN and Z.-L. ZHANG. Optimal forwarder list selection in opportunistic routing. In: *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009*. Macau: IEEE, 2009, pp. 670–675. ISBN 978-1-4244-5113-5. DOI: 10.1109/MOBHOC.2009.5336939.

[7] KURTH, J.-P., A. ZUBOW, and J.-P. REDLICH. Cooperative opportunistic routing using transmit diversity in wireless mesh networks. In: *The 27th Conference on Computer Communications*. Phoenix: IEEE, 2008, pp. 1310–1318. ISBN 978-1-4244-2025-4. DOI: 10.1109/INFOCOM.2008.188.

[8] LU, M., LI, F. and J. WU. Efficient opportunistic routing in utility-based ad hoc networks. *IEEE Transactions on Reliability*. 2009, vol. 58, iss. 3, pp. 485–495. ISSN 0018-9529. DOI: 10.1109/TR.2009.2020100.

[9] DUBOIS-FERRIERE, H., M. GROSSGLAUSER and M. VETTERLI. Least-cost opportunistic routing. In: *Proceedings of Allerton Conference on Communication, Control, and Computing, 2007*. Illinois: University of Illinois at Urbana-Champaign, 2007, pp. 1–8. ISBN 978-1605600864.

[10] GOVINDAN, K. and P. MOHAPATRA. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey. *IEEE Communications Surveys & Tutorials*. 2012, vol. 14, iss. 2, pp. 279–298. ISSN 1553-877X. DOI: 10.1109/SURV.2011.042711.00083.

[11] TRIFUNOVIC, S., F. LEGENDRE and C. ANASTASIADES. Social trust in opportunistic networks. In: *INFOCOM IEEE Conference on Computer Communications Workshops*. San Diego: IEEE, 2010, pp. 1–6. ISBN 978-1-4244-6739-6. DOI: 10.1109/INFCOMW.2010.5466696.

[12] OPNET Modeler Simulation Software. *Riverbed* [online]. 2012. Available at: `http://www.opnet.com`.

About Authors

Jan PAPAJ was born in Liptovsky Mikulas, Slovak Republic in 1977. He is graduated at the Department of Computers and Informatics in 2001, Faculty of Electrical Engineering and Informatics at Technical University in Kosice. He obtained his Ph.D. degree in Telecommunications from the Faculty of Electrical Engineering, Technical University of Kosice in 2010. His research interests cover the fields of mobile ad-hoc networks, QoS and security, context and content routing protocols, opportunistic networks, delay tolerant networks, sensor networks.

Lubomir DOBOS was born in Vranov nad Toplou, Slovak Republic in 1956. He received the Ing. (M.Sc.) degree and Ph.D. degree in Radioelectronics from the Faculty of Electrical Engineering, Technical University of Kosice, in 1980 and 1989, respectively. He defended his habilitation work - Broadband Wireless Networks for Multimedia Services in 1999. His scientific research area is: adaptive noise cancellations in speech, broadband information and telecommunication technologies, multimedia systems, telecommunications networks and services, universal mobile communication systems (UMTS), 5G networks.