International Journal of Business Data Communications and Networking
Volume 17 • Issue 2

A New Cooperation Model for Dynamic Networks

Mohamed Amine Riahla, LMOSE Laboratory, Boumerdes University, Algeria*

Sihem Goumiri, Ingénierie des Systèmes et Télécommunications Laboratory, University of Boumerdes, Algeria

Karim Tamine, Limoges University, France

M'hamed Hamadouche, LIMOSE Laboratory, University of Boumerdes, Algeria

https://orcid.org/0000-0001-8505-3715

ABSTRACT

Technological evolution has revealed new types of dynamic networks with decentralized architectures and autonomous services. Research on this impressive area has provided great objectives and benefits. However, providing some services related to security and routing protocols are major problems in this domain. All nodes in the networks need to cooperate and relay packets for other nodes, but some misbehaving nodes due to selfish reasons may significantly reduce the network performances. In this paper, a novel technique of enforcement cooperation is proposed. It aims to control the role of each node in the network and evaluate their participation during the routing function. The model includes important features that force node cooperation and discard the selfish ones. Simulation results showed that the proposed model is efficient in detecting and removing misbehaving nodes and enhancing cooperation between nodes while routing data.

KEYWORDS

Cooperation Enforcement Model, Dynamic Networks, MANET, Reputation System, Routing Data, VANET, WSN

INTRODUCTION

A distributed dynamic network (Tariq et al., 2019; Al-Sakib, 2016) is a self-organized system without any central management infrastructure; it gathers a set of mobile nodes connected with wireless links. Topologies in these networks are always in a dynamic change due to the frequent movement of nodes. Various categories of dynamic networks are referred to as: Ad hoc (Manets: Mobile Ad Hoc Networks) (Al-Sakib, 2016; Raza et al., 2016; Pushpa & Kathiravan, 2016), VANETs (Vehicular Ad-Hoc Network) (Hamdi et al., 2020; Liu et al., 2016; Zhang et al., 2013), VMN (Wireless Mesh Network) (A. Nanda et al., 2020; Al Islam et al., 2016) and WSN (Wireless Sensors Network) (Elhoseny & Hassanien, 2019; Kaur et al., 2016) .

Deploying these networks is quick and spontaneous at a low cost. However, providing some services like security and routing could be a veritable challenge. Most existing routing protocols supposed that all nodes co-operate in the network to forward packets, but constraints in bandwidth, storage, and energy power in mobile devices revealed uncooperative nodes, which use resources for their own purpose. These nodes have a selfish behavior that disrupts communications between other nodes and reduces the network performances.

DOI: 10.4018/IJBDCN.286704

*Corresponding Author

A system of cooperation enforcement is strictly required when deploying the network. Authors in (Khan et al., 2018; Mantas et al., 2017) have classified cooperation systems into two categories; these are Reputation-based Methods and Credit-based Methods. The first one is based on calculating the reputation between nodes like applied in CONFIDANT (Buchegger & Le Boudec, 2002a; Buchegger & Le Boudec, 2002b; Buchegger & Le Boudec, 2004) and SORI (He & Le Boudec, 2002). The second one employs the concept of credit between nodes like used in the protocols TOKEN BASED (Yang et al., 2002) and SPRIT (Yang et al., 2003). These categories are explained further in the paper with more details.

The current study proposes an efficient reputation-based approach that enhances cooperation and discards selfish nodes. The main objective here is to make a distributed collective decision between nodes to insulate a misbehaving node for a predefined duration. As a second objective, the model allows reinserting the punished node again to the network after expiring its punishment time. Therefore, it offers a second chance to the misbehaved nodes to be more collaborative in the network. The proposed solution is designed according to the distributed and random characteristics of dynamic networks. Therefore, it can be easily integrated into any routing protocol designed for these networks. The remaining part of the paper is organized as follows:

In section 2, previous works related to cooperation models in dynamic networks are presented. In section 3, the functionalities of the proposed model are explained with technical details. Section 4 illustrates the experimental evaluation of comparison results using the NS2 3 simulator, this section involves the performance of the proposed solution based on different metrics. The paper ended with future works a conclusion and perspectives.

BACKGROUND

Cooperation Models in Dynamic Networks

The cooperation system is essential to build collaborative relationships between nodes in a network. The main reason for this concept is to motivate participation in the network functions and enhance its performances. The cooperation system is also defined as a component of security that observes misbehavior nodes in the network. In general, existing cooperation models are classified into two distinct categories: reputation-based models and credit-based models (Khan et al., 2018; Mantas et al., 2017). In the current state of the art, the cooperation models in dynamic networks are numerous and varied. Our focus has been to survey the first basic models that existed in literature and inspired many recent models.

Reputation-Based Models

The system evaluates the node behavior by computing its reputation in the network. Each node reports information about neighboring reliability before establishing communication. The reputation value is calculated based on the effective participation of a node in the routing function: When a node collaborates in neighboring data transfer, the system increases its reputation value and vice versa. Uncooperative nodes with low reputation values are detected and isolated from the network. Several existing models have implemented this method like CONFIDANT (Buchegger & Le Boudec, 2002; Buchegger & Le Boudec, 2002;Buchegger & Le Boudec, 2004), SORI (He & Le Boudec, 2002); OCEAN (Dewan et al., 2003)and CORE (Pietro & Le Refik, 2002).

CONFIDANT (COoperation of Nodes, Fairness In Dynamic Ad-hoc NeTworks) was proposed in different versions. This paper involves the basic operating idea of CONFIDENT introduced in the works of Buchegger and Le Boudec (Buchegger & Le Boudec, 2002). The authors suggested a cooperative approach to insulate selfish nodes in the network, thus, achieving both the correctness and efficiency of routing packets. The method was implemented with the DSR (Jain, 2016; Chao, 2016, pp. 6878-6882) routing protocol to evaluate cooperation between nodes. Each node in the network uses four schemes in an interaction called: the monitor, the reputation system, the trust management, and the route management.

The monitor observes and evaluates nodes' behavior during the routing process. The obtained observations are sent to the reputation system, which is responsible for updating reputation values for each observed node. The trust management scheme is a powerful tool to detect misbehavior nodes efficiently in the network. By taking into account the previous observations, this system provides decisions about a node's behavior. It uses negative remarks between nodes and their neighbors to identify misbehavior nodes. Trust management is also responsible for sharing the reputation values over the whole network. The last component used by CONFIDENT is route management. Its main goal is to find the optimal routes through reliable nodes and avoid routing packets of all nodes having a low reputation value (below the level of CONFIDENT tolerated value).

Same to CONFIDENT, SORI (Secure and Objective Reputation-based Incentive) (He & Le Boudec, 2002) is a system for detecting uncooperative nodes during the routing process. Except, it limits observations by one hop and calculates the reputation of nodes in local neighboring areas. Nodes executing this protocol proceed as follow:

Firstly, node N maintains a local list of neighbors with one hope (x1, x2…xn). When this node transmits packets, it saves a first parameter related to the number of packets that each neighbor X should forward. As a second parameter, it observes the total number of packets sent by each neighbor. Based on these two parameters, node N calculates the reputation value of its neighbors. The trustworthiness of node N for its neighboring judgments is evaluated based on its trust level value. After that, the node N creates a local recode including the behavior of each neighbor X. records are periodically updated, and in the case of the reputation value is significantly changed, the updated record is forwarded to all neighbors. To have a global observation about the neighbor x, node N uses another record including all neighbors' observations about the node x behavior.

Moreover, SORI proposed an additional security scheme. It includes authentication of reputation messages by using the protocol TESLA (Verma et al., 2003; Benmachiche et al., 2016). This approach was implemented in the same manner as used in the protocol ARIADNE (Yih-Chun Hu et al., 2005).

Credit-Based Models

The second model to enhance cooperation between nodes is based on credit. In this model, some services like rooting are performed with the appropriate payment. The system includes virtual money to control traffic between nodes. All the nodes (senders and, or receivers) that benefit from the network must pay the intermediate nodes participating in the routing function. Many existing operational systems have implemented this method like TOKEN BASED (Yang et al., 2002), Sprit (Yang et al., 2003), and ad hoc-VCG (Anderegg & Le Eidenbenz, 2003).

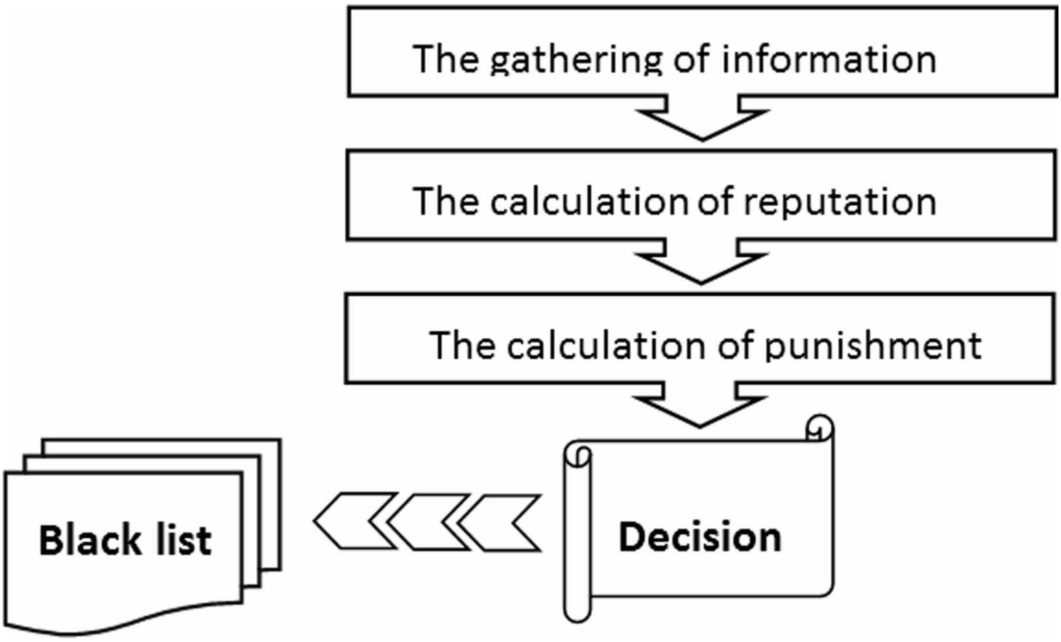
TOKEN-BASED (Yang et al., 2002) defines a token with a limited period for each node newly connected to the network. In this period, the node is observed by its neighbors to detect any misbehaving action. Once the token period is expired, the node must request its neighbors to be reinserted to the network. The term validity of tokens depends on the time of nodes' participation in the network.

PROPOSED MODEL

We propose in this paper a model based on cooperation enforcement in a dynamic network. The system was integrated with a routing protocol to provide novel functions that detect and punish misbehavior nodes. The concept is based on calculating the reputation values of nodes through local and extern observations between neighbors. This process enhances cooperation and built over time a trust relationship in the network. The proposed model blends four modules listed below and illustrated in figure 1:

- The gathering of information

Figure 1. The modules of the proposed model


The gathering of information
The calculation of reputation
The calculation of punishment
Black list
Decision

- The calculation of reputation
- The calculation of punishment
- The final decision

The following paragraphs summarize the operation idea steps by step of the proposed solution:

The protocol creates an agent called « RéputationAgent» for each network node to monitor its neighbor nodes in a promiscuous mode. Monitoring allows examining the network traffic while forwarding and receiving packets between nodes. The promiscuous mode permits node (N) to calculate the reputation value of its nearby node (Nm) (that it monitors) over each period over time. The obtained reputation value will then deliver the decision about the punishment of the neighbor (Nm). This decision is a stochastic function detailed further in the paper.

Node (N) punishes the neighbor node (Nm) while obtaining an affirmative punishment decision about this neighbor associated with its reputation history. The punishment time is a period delivered by the probability function. In this situation, the system avoids all data routing packets passing through the node (N) to achieve the punished node (Nm). Therefore, the punished node will have a routing table rarely updated, notably when other neighbors have applied the same decision. Over time, nodes discard the punish node (Nm) from the network due to the decreased number of routes in its routing table.

The system performs a distributed decision-making process over all the nodes in the network. For each time that a node misbehaves, its reputation value decreases around other nodes. Therefore, the proposed model is totally decentralized and well adapted to any routing protocols for dynamic networks.

THE DETAILED OPERATION OF THE COOPERATION MODEL

This section presents the operation of the proposed model with technical details. The modules of the solution defined previously will be described in detail and illustrated with equations and figures.

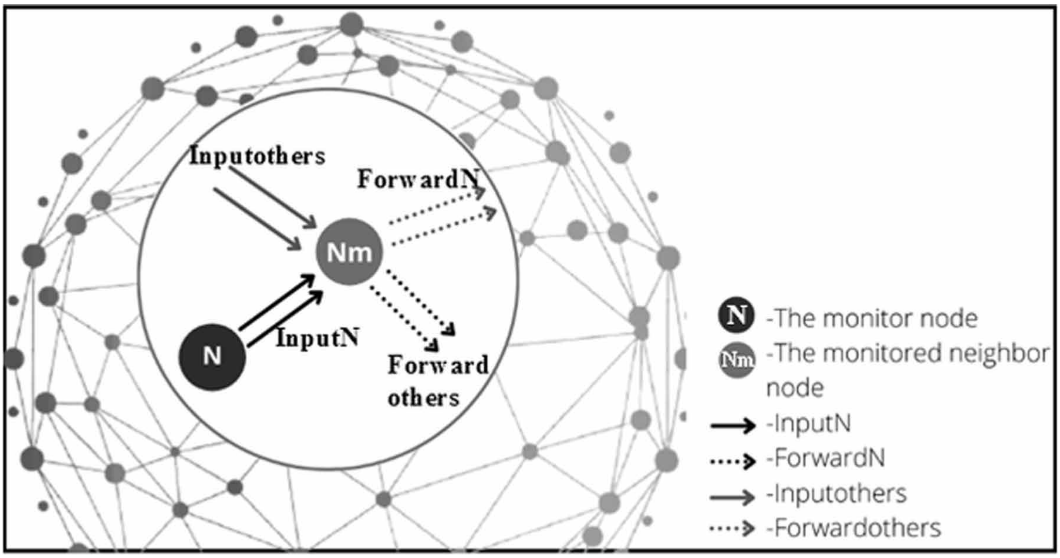
1. The gathering of information

Periodically over time, as described above, every node in the network monitors its neighbors during the routing process; observations focus on forwarding the received packets. The monitoring controls some parameters collected when each node (N) monitors its neighbor node (Nm). These parameters are defined as follows:

Input$_N$: Defines the number of packets sent by the node (N) to its neighbor (Nm) which it must forward.
Forward$_N$: Defines the total number of packets sent by the node (N) and forwarded by the neighbor (Nm).
Input$_{others}$: Defines the number of packets sent by other nodes (other than node N) to the node (Nm which it must forward.
Forward$_{others}$: Defines the total number of packets sent by the other nodes (other than node N) and forwarded by the node (Nm).

We notice that monitoring operates in the promiscuous mode (i.e., accept all received messages despite those destined to other nodes). We also mention that nodes can intercept all transiting messages in the coverage zone because communications are established with wireless links.

Figure 2. The operation of monitoring process



2. The calculation of reputation

After the monitoring process, the node calculates the reputation value (NR) for each neighbor node figuring in its routing table. Saving this information allows the node to transmit its data packets through trusted nodes. A neighbor with a trust state means that its reputation value (NR) is strictly higher than the level set by the protocol. The node uses two values to calculate the reputation value (NR): the direct reputation value and the extern reputation value, as described by the following.

a. The direct reputation value:

The direct reputation value is related to the local monitor of node N about its neighbor node Nm. This value is based on the previous parameters collected in the monitor process as shown in equation (1):

$$DRV\left(N, N_m\right) = \alpha \frac{farward_N}{input_N} + \left(1-\alpha\right)\frac{farward_{other}}{input_{other}} \quad with \quad 0.5 < \alpha < 1 \,. \tag{1}$$

Where:

N is the monitor node
N_m is the monitored neighbor node
DRV (N, Nm) is the direct reputation value attributed by node N to its neighbor N_m.
$Input_N$, $Forward_N$, $Input_{others}$, and $Forward_{others}$ are the parameters obtained previously from the gathering information module.

The ratio $\frac{farward_N}{input_N}$ .efines the packets' forwarded rate by node N_m, relative to the total number of packets received by node N_m from node N.

The ratio $\frac{farward_{other}}{input_{other}}$ .efines the packets' forwarded rate by node N_m, relative to the total number of packets received by node N_m from the other neighbors.

α factor plays the main part in defining the behavior of node N_m. It presents the weightage that controls the ratios $\frac{farward_N}{input_N}$ .nd $\frac{farward_{other}}{input_{other}}$. This value is between 0.5 <α< 1 as shown in equation (1). When α>0.5 it means that the system promotes the first ratio in the equation. Otherwise, the second ratio is taken into consideration. This designates which observations are taken into account, those of the monitor node N or those of the other neighbors. The system, before valuing nodes, respects the reason why a node refuses to forward the sent packets. It may be that the monitored node does not forward packets coming from a selfish neighbor. Therefore, the factor α minimizes the impact of bad judgments on the reputation value of the monitored nodes.

b. The extern reputation value

The proposed solution includes several scenarios in the network. Supposing that a node isolates a misbehavior neighbor node, and this one changes its location to still benefiting from services. In this situation, the system requests the extern reputation value to diffuse that information throughout the network. This value gathers all recommendations between the whole network nodes and defines the trusted relationships. Such a characteristic makes the model totally distributed and well adapted to the nature of dynamic networks. The extern reputation value is calculated by using the reputation values received from other nodes in the network. We notice that the calculation only considers recommendations of the trusted nodes. The extern reputation value of the node (i) about the node (j) is calculated as shown in equation (2):

$$\mathbf{Next}\left(\mathbf{i},\mathbf{j}\right)=\frac{1}{\left|\mathbf{N}_{\mathbf{j}}\right|}\sum_{\mathbf{k}\in\mathbf{N}_{\mathbf{j}}}\mathbf{DRN}\left(\mathbf{k},\mathbf{j}\right)\times\mathbf{RN}\left(\mathbf{i},\mathbf{k}\right). \tag{2}$$

Equation (2) is a general average of distributed decisions. It determines the node (i) judgment about the node (j) behavior according to trusted node decisions where:

Next (i,j) is the extern reputation value attributed by the node i to the node j.

N(j) is a set of nodes existing in the trust table of the node (i) and having a trust value about the node (j). Nodes belonged to N(j) must have a reputation value RN greater or equal to the level set in the trust table of the node (i).

DRN(k,j) is a reputation value attributed by trusted nodes k $(k \in N_j$. to the node (j)

RN (i, k) is the reputation value of the node (k) known at node (i); it must be equal or greater than the level value in the trust table of the node (i) in order to take into consideration only trusted nodes recommendations.

c. The final reputation value

The final reputation value evaluates the trust level between two nodes (i) and (j). It is obtained based on the direct and the indirect reputation values, and calculated as shown in (3):

$$\mathbf{RN}_{\mathbf{t}}\left(\mathbf{i},\mathbf{j}\right)=\frac{\pm\mathbf{RN}_{\mathbf{t}-1}+\left[{}^{2}\,\mathbf{DRV}_{(\mathbf{i},\mathbf{j})}+\left(1-{}^{2}\right)\mathbf{next}\left(\mathbf{i},\mathbf{j}\right)\right]}{1+\pm}\mathbf{whith}\quad 0<\pm<0.5\,\mathbf{and}\,0.5<{}^{2}<1. \tag{3}$$

Where:

RN$_t$ (i,j) is the final reputation value attributed by node (i) to the node (j) at the moment t,

RN$_{t-1}$ is the precedent final reputation value of node (j),

DRV $_{(i,j)}$ is the direct reputation value attributed by node (i) to the node (j),

next$_{(i,j)}$ is the extern reputation value attributed by node (i) to the node (j).

The parameters α and β are the weights in this equation. The α value is between 0 and 0.5, when α>0 the system regularly forgets older monitoring. This case is observed when a node is no longer selfish and correctly participates in the routing function. The β value is used for providing greater importance to the direct reputation value DRV $_{(i,j)}$, and less importance to the extern reputation value next$_{(i,j)}$. β >0 allows a node to promote its observations to have more than the other nodes' observations.

The proposed solution also examines inactive nodes in the network. Although their behavior was good before disconnection from the network, their direct reputation value decreases over time. Such a condition avoids a node to long benefit from its old trusted character. The system decreases its reputation value until reaching the 0.5 value that defines a neutral behavior. A node newly inserted in the network is considered as trusted node with the direct reputation value DRN=1.

We notice that all trust values (NC) are evaluated in the range of [0, 1], 0 <= NC(x, y) <= 1.

3. The punishment

Table 1. Simulation parameters

Parameter	Value
Simulation time	0-500 s
Packet size	512 bits
Number of nodes	500 nodes
Number of data packets	1000 packets
MAC Type	IEEE 802.11 b
Simulation area	1000 m2
Traffic	FTP
Mobility model	Random way point
Receiving range	100 m
Propagation model	Two ray ground
Packet rate	16 Packets/sec
Node speed	5-30 m/s
The α value	0.5
The k value	100

After the processes of observation and allocating reputation values, a node make a punishment decision about the selfish node. A period (t) proportional to the value p defines the duration of isolating the punished node from the network. The value p is a probabilistic function with p=1-RN.

During the penalization time (t) the punished node is block listed. In this period, the system avoids transiting all control packets that update its routing table, which minimizes the number of routes in this table.

To prevent the punished node from establishing routes using its control packets; the other nodes automatically delete each message received from this node. Consequently, it will be isolated from the network over time.

The proposed punishment scheme enhances cooperation between nodes to benefit from the network services. After the expiration of the punishment time, the system gives a second chance for the punished node. This node is deleted from the block list and will be operational in the network.

SIMULATION PARAMETERS

We used the NS2 simulator to evaluate the performance of our proposed algorithm. The parameters considered in the simulation are shown in Table 1.

The traffic is created randomly and generated automatically by a (Tcl) script mainly developed for this purpose.

The implementation of the proposed system is illustrated in figure 3. For each period t, a node creates a local agent to calculate reputation values basing on the collected information. After that, the agent will calculate the penalizations and save all the obtained values in its reputation table. For the penalization time value, a node uses a function proportional to (p) with penalization (p)= kp (where k is a positive real).

First simulation tests were based on studying the node N behavior (N is chosen randomly from the network) and those of its neighbors in the following two cases:

- The node N is not a selfish node
- The node N is a selfish node

The performance metrics are obtained by averaging over 30 simulation runs as described in the following:

1. The number of nodes that consider the monitored node as a neighbor:

This metric defines the neighbors of the monitored node, which they considered a trusted node. Such a metric demonstrates if the network nodes consider the trust dimension while choosing routes.

2. The number of neighbors in the routing table of the monitored node:

This metric indicates the cooperation state of the monitored node with other network nodes.

SIMULATION RESULTS

The Number of Neighboring Nodes with the Monitored Node

When node N is selfish, the analyses indicate that the number of nodes reached by this node diminishes over time. Unlike when it is not selfish, the number of nodes decreases. Consequently, some nodes had previously judged and penalized this selfish node. However, after some time, the number of nodes reached by node N rises gradually due to the second chance mechanism provided by the system. Indeed, after the expiration of the penalization delay, node N is functional again in the network.

Results showed in figure 4 approve the effect of the proposed model on the network nodes. As illustrated, limited routes are established with selfish node because nodes cooperate only with unselfish nodes. The selfish ones are penalized and do not benefit from the network resources and services.

The Number of Neighbors in the Routing Table of the Monitored Node

The following figures show the monitored node activities in the network. In advance, we defined the number of neighbors in the routing table of the monitored node.

Figures 5 and 6 show the number variation of neighboring nodes in the routing table of the monitored node over time.

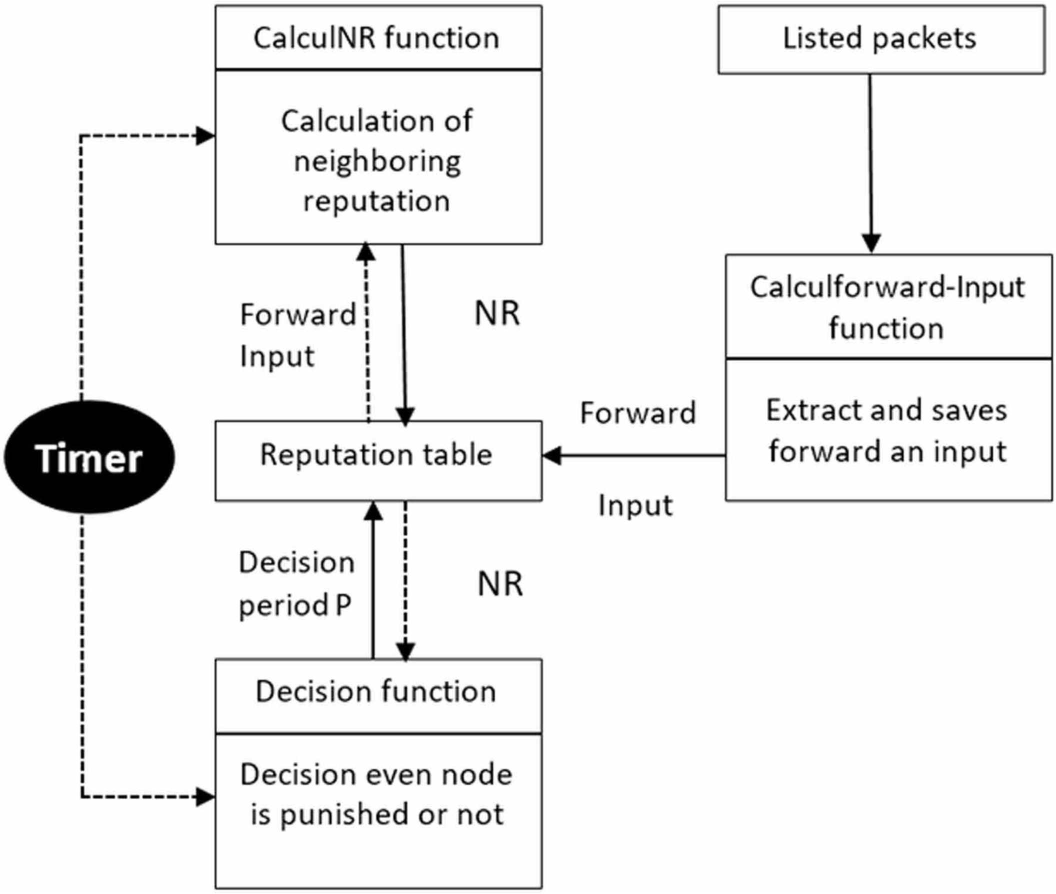
At the beginning of the simulation, whatever node N behavior is selfish or trusted, its routing table initially contains the same number of neighbors. Once node N misbehaves in the network with selfishness, the number of its neighbors decreases until reaching the value 0, as shown in figure 6. The graph so affirms that this node is punished and isolated from the network by its neighbors. After some time, the graph takes another direction indicating that the routing table of node N saves more neighbor nodes. Thus, the node is unblocked in the network after the expiration of penalization time. In this case, it benefits from the network resources and services; and neighbors restart routing its packets.

Observations from simulation results showed that the proposed system performs the process related to discarding selfish nodes from the network. The second chance system encourages selfish nodes to behave correctly and reinforces cooperation between nodes.

FUTURE WORKS

For many Years research in dynamic and self-organized networks has continually provided significant results, but still insufficient with the rapid technologies evolution. In the current paper, we present a solution to enhance cooperation in dynamic networks that give direction to the researchers in this area.

Figure 3. The implemented tables describing the proposed model structure


CalculNR function
Calculation of neighboring reputation
Listed packets
Forward Input
NR
Calculforward-Input function
Extract and saves forward an input
Forward
Timer
Reputation table
Input
Decision period P
NR
Decision function
Decision even node is punished or not

Concerning future research, our focus will be on increasing the level of security in these networks based on new tools and methods introduced in the literature. In addition, we are encouraged to develop and integrate the proposed model into different networks like VANET and FANET.

CONCLUSION

The current study explores the selfish nodes problem in dynamic networks. We have proposed a cooperation-based model implemented with an existing routing protocol. The main goal of this study is to enhance cooperation between nodes, which ensures the routing task and increases the security level in networks. Based on new techniques and notions, the model accurately identifies and isolates selfish nodes. The network nodes perfectly applied the process of observation, and attributed reputation values between them, which allow defining selfish nodes. Obtained graphs indicated that the network nodes could applied all necessary decisions to punish selfish node for a probabilistic period.

The second chance mechanism implemented with the solution provides significant results in simulations. Indeed, experimental and simulation results demonstrate that misbehaving nodes have changed their selfish behavior and collaborate correctly in the network after their first punishment.

For more performance, our focus will be on implementing the extern reputation value detailed previously. This perspective allows monitoring the mobility of selfish nodes in the network.

Figure 4. The variation of the monitored node neighbors in 200 s simulation time

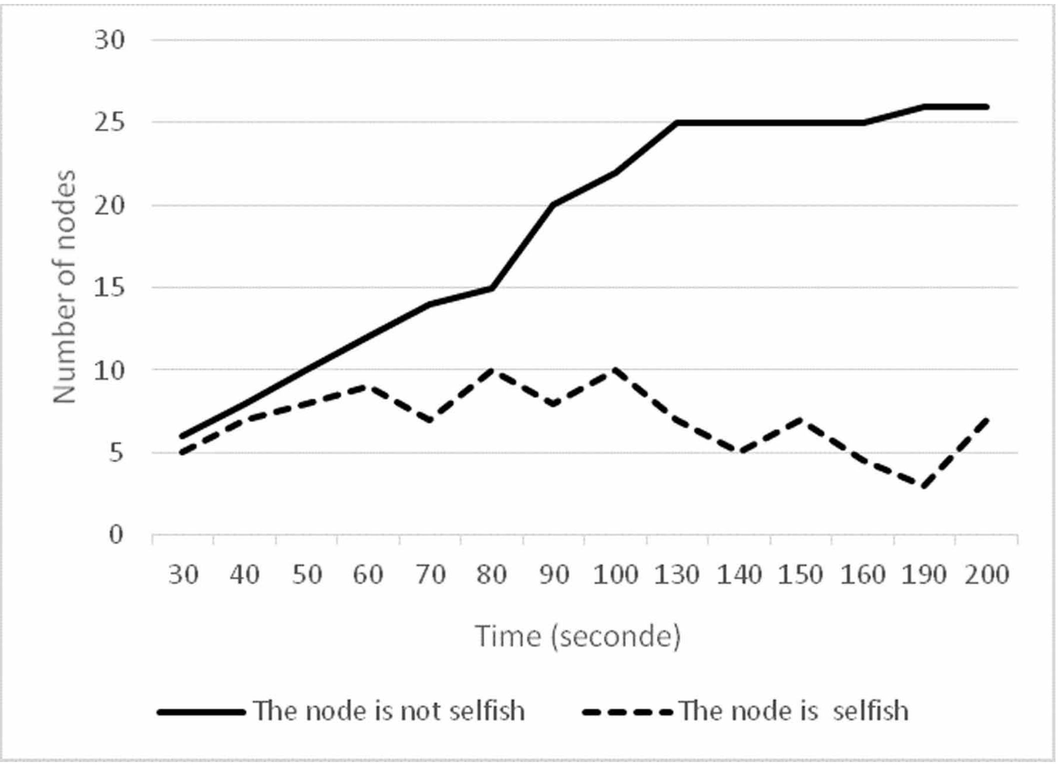


Figure 5. The number variation of neighboring nodes in the routing table of the monitored node over time

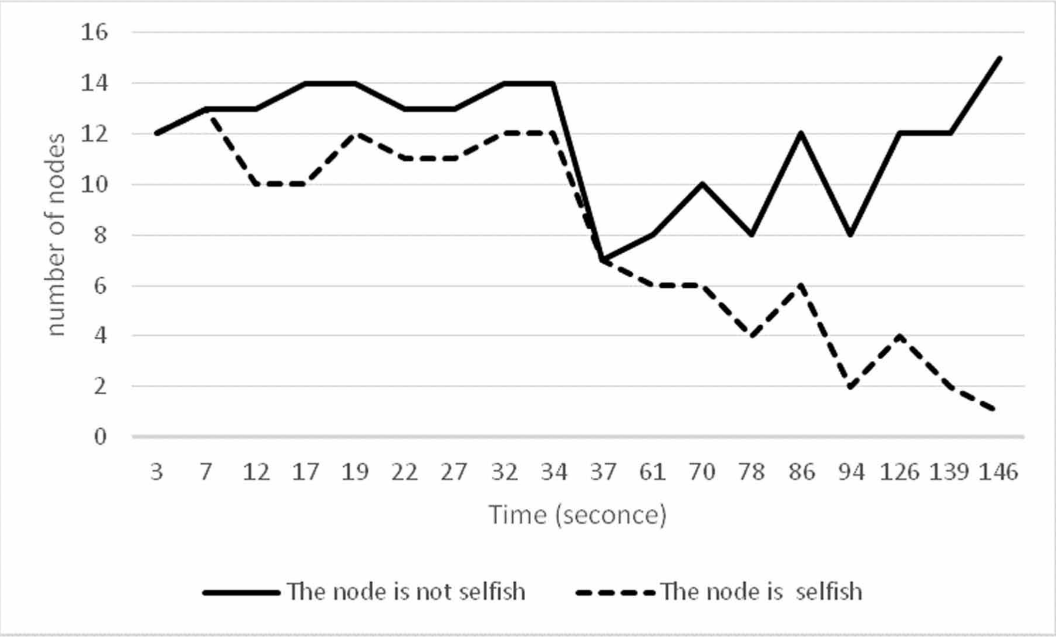
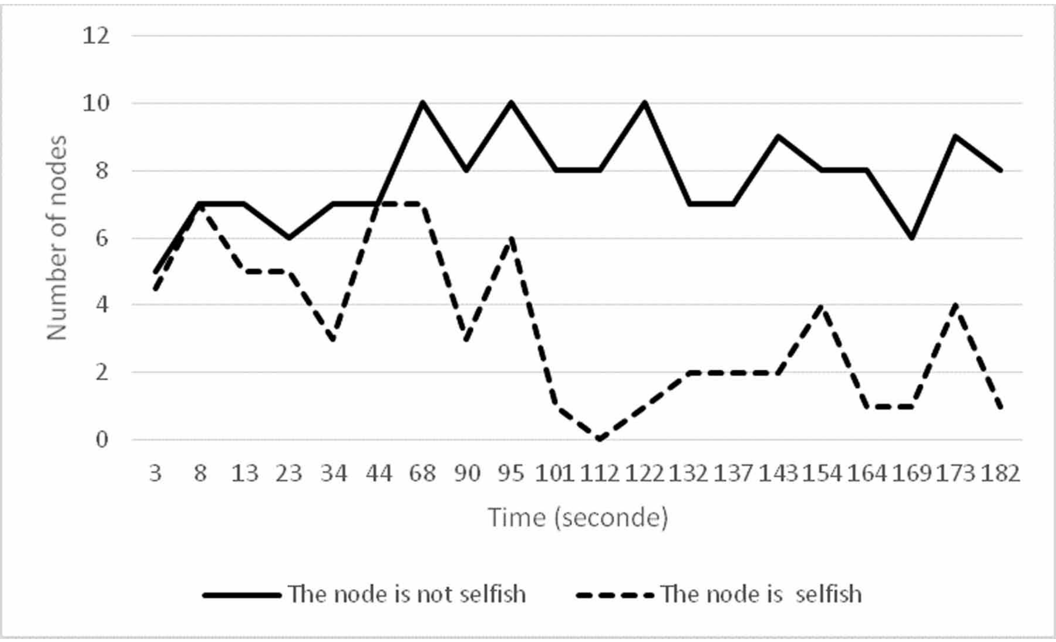


Figure 6. The number variation of neighboring nodes in the routing table of the monitored node over time (the monitored node is being collaborative after its first penalization)



This paper is an initial work implementing a cooperation model. We suggest future researches that expand the implementation spectrum of our solution. Thus, we plan to integrate our reputation model in other dynamic networks as FANET and FANET.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

Funding Statement

No funding was received for this work.

Process Dates:

Received: January 23, 2021, Revision: July 30, 2021, Accepted: August 3, 2021

Corresponding Author:

Correspondence should be addressed to Mohamed Amine Riahla, ma.riahla@univ-boumerdes.dz

REFERENCES

Al Islam, A. A., Islam, M. J., Nurain, N., & Raghunathan, V. (2016). Channel Assignment Techniques for Multi-Radio Wireless Mesh Networks: A Survey. *IEEE Communications Surveys and Tutorials*, *18*(2), 988–1017. doi:10.1109/COMST.2015.2510164

Al-Sakib Khan Pathan. (2011). *Security of Self-Organizing Networks MANET, WSN, VMN, VANET*. CRC Press Taylor & Francis Group.

Anderegg, L., & Eidenbenz, S. (2003). Ad hoc-VCG: a Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents. *Proceedings of 9th Annual International Conference on Mobile Computing and Networking*, 245-259. doi:10.1145/938985.939011

Benmachiche, A., Ali, S., & Messikh, A. (2016). A source authentication and data confidentiality scheme based on TESLA protocol and XOR encryption for multicast. *International Journal on Perceptive and Cognitive Computing*, *2*(2). Advance online publication. doi:10.31436/ijpcc.v2i2.23

Buchegger, S., & Le Boudec, J.-Y. (2004). Self-policing mobile ad hoc networks. In M. Ilyas & I. Mahgoub (Eds.), *Mobile Computing Handbook, pages 435Ŕ456*. CRC Press.

Buchegger, S., & Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks). In *Proceedings of the Third ACM International Symposium on Mobile ad hoc Networking and Computing*. ACM Press.

Buchegger & Le Boudec. (2002). Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM.

Chao, T. (2016, July). LAR routing stability protocol based on mobility prediction. In *Control Conference (CCC), 2016 35th Chinese* (pp. 6878-6882). TCCT. doi:10.1109/ChiCC.2016.7554440

Ciobanu, R. I., Negru, C., Pop, F., Dobre, C., Mavromoustakis, C. X., & Mastorakis, G. (2019). Drop computing: Ad-hoc dynamic collaborative computing. *Future Generation Computer Systems*, *92*, 889–899. doi:10.1016/j.future.2017.11.044

Dewan, P., Dasgupta, P., & Bhattacharya, A. (2004, July). On using reputations in ad hoc networks to counter malicious nodes. In *Proceedings. Tenth International Conference on Parallel and Distributed Systems, 2004. ICPADS 2004* (pp. 665-672). IEEE. doi:10.1109/ICPADS.2004.1316153

Elhoseny, M., & Hassanien, A. E. (2019). Dynamic wireless sensor networks. In Studies in Systems, Decision and Control (Vol. 165). Springer International Publishing AG. doi:10.1007/978-3-319-92807-4

Hamdi, M. M., Audah, L., Rashid, S. A., Mohammed, A. H., Alani, S., & Mustafa, A. S. (2020, June). A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-7). IEEE.

He, Q., Wu, D., & Khosla, P. (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. In *Proceedings of the Third IEEE Wireless Communications and Networking Conference, WCNC 04* (vol. 2, pp. 825-830). IEEE Press.

Hu, Y.-C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, *11*(1-2), 21–38. doi:10.1007/s11276-004-4744-y

Jain, A. (2016). Performance Analysis of DSR Routing Protocol With and Without the Presence of Various Attacks in MANET. *International Journal of Engineering Research and General Science*, *4*(1).

Kaur, J., Gill, S. S., & Dhaliwal, B. S. (2016). Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks. *Journal of Engineering (Stevenage, England)*.

Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., & Yaacob, M. (2018). A survey on MANETs architecture, evolution, applications, security issues and solutions. *Indonesian Journal of Electrical Engineering and Computer Science*, *12*(2), 832–842. doi:10.11591/ijeecs.v12.i2.pp832-842

Liu, J., Wan, J., Wang, Q., Deng, P., Zhou, K., & Qiao, Y. (2016). A survey on position-based routing for vehicular ad hoc networks. *Telecommunication Systems, 62*(1), 15-30.

Mantas, N., Louta, M., Karapistoli, E., Karetsos, G. T., Kraounakis, S., & Obaidat, M. S. (2017). Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: A survey. *IET Networks*, *6*(6), 169–178. doi:10.1049/iet-net.2017.0079

Michiardi & Molva. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, (pp. 107-121). Kluwer, B.V.

Nanda, A., Nanda, P., He, X., Jamdagni, A., & Puthal, D. (2020). A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks. *Future Generation Computer Systems*, *109*, 521–530. doi:10.1016/j.future.2018.05.065

Pushpa, A. M., & Kathiravan, K. (2016). A comparative survey of security solutions for multicast and unicast routing protocols in mobile ad hoc networks. *International Journal of Wireless and Mobile Computing*, *10*(3), 232–249. doi:10.1504/IJWMC.2016.077221

Raza, A., Al-Karaki, J. N., & Abbas, H. (2016). Analyzing Packet Forwarding Schemes for Selfish Behavior in MANETs. In Information Technology: New Generations (pp. 227-236). Springer International Publishing. doi:10.1007/978-3-319-32467-8_21

Tariq, A., Rehman, R. A., & Kim, B. S. (2019). Forwarding Strategies in NDN-Based Wireless Networks: A Survey. *IEEE Communications Surveys and Tutorials*, *22*(1), 68–95. doi:10.1109/COMST.2019.2935795

Verma, J., Shukla, P. K., & Pandey, R. (2016). Survey of various Trust based QoS aware Routing Protocol in MANET. *Traffic, 137*(3).

Yang, H., Meng, X., & Lu, S. (2002). Self-Organized Network-Layer Security in Mobile ad hoc Networks. *Proceedings of the 1st ACM workshop on Wireless security*, 11-20. doi:10.1145/570681.570683

Zhang, D., Huang, H., Zhou, J., Xia, F., & Chen, Z. (2013). Detecting hot road mobility of vehicular Ad Hoc networks. *Mobile Networks and Applications*, *18*(6), 803–813. doi:10.1007/s11036-013-0467-6

Zhong, S., Chen, J., & Yang, R. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. Proceedings of IEEE INFOCOM2003. doi:10.1109/INFCOM.2003.1209220

Mohamed Amine Riahla is Computer Science Teacher at the University of Boumerdès (Algeria) since November 2008. He received the Ph.D. degree in computer sciences from University of Limoges (France) and the HDR degree from University of Boumerdes (Algeria). His research and teaching interests are in artificial intelligence applied to security of dynamic networks (Drones, ad hoc, VANET, mesh, Iot and sensor networks). Currently, he is working on routing, security and privacy in cloud and dynamic networks.

Sihem Goumiri is a second year Phd student at University of Boumerdes (Algeria), Faculty of technologies at the telecommunication Department. For her PhD Thesis, she is working under the routing and security challenges in the dynamic and autonomous networks (Drones, ad hoc, VANET, mesh, IoT and sensor networks).

Karim Tamine is an Associate Professor of Computer Science and Engineering at the University of Limoges (France) since September 1997. He received the Ph.D. degree and DEA in computer sciences from University Paul Sabatier (Toulouse, France). His research and teaching interests are in artificial intelligence applied to computer graphics and security of wireless ad-hoc and sensor network. Currently, he is working on multicast routing, quality of service, intrusion detection, security, and privacy in P2P networks. He has several refereed international publications (journals and conferences) in all these domains.

M'hamed Hamadouche was born in Relizane, Algeria, on January 18, 1954. He received the Ph.D. degree in electrical engineering, on January 16, 2001, from University of Constantine, Algeria. He is currently a professor at University M'hamed Bougara of Boumerdes, Algeria and associate professor at High School of Air defense, in signal processing. His main research interests are Radar detection, Detection and estimation, Coding and Cryptology.