Social CLWPR: A Socially enhanced Position based Routing Protocol for handling misbehaviour inVANETs

Nikolaos Mantas
Informatics and Telecommunications Engineering
School of Engineering,
University of Western Macedonia
Kozani, Greece
nmantas@uowm.gr

Malamati Louta
Informatics and Telecommunications Engineering
School of Engineering,
University of Western Macedonia
Kozani, Greece
louta@uowm.gr

Konstantinos Katsaros
Institute for Communications Systems
Department of Electronic Engineering, University of Surrey
Guildford, United Kingdom
K.Katsaros@surrey.ac.uk

Stylianos Kraounakis
Informatics and Telecommunications Engineering
School of Engineering,
University of Western Macedonia
Kozani, Greece
skraounakis@yahoo.gr

***Abstract*— In this paper, we enhance CLWPR, a cross-layer optimized position-based routing protocol for urban VANET environments, introducing social aspects to its design so as to efficiently address misbehaving (selfish or malicious) nodes that intentionally drop packets and ultimately promote cooperation in the network. The proposed Social CLWPR protocol favors nodes with close favorable social relationship (family members, friends, users with trust connections) as next forwarder nodes, while nodes with explicit distrust connections as indicated from online social media are not preferred in the network. Social CLWPR performance is comparatively evaluated against CLWPR and it demonstrates improved performance in terms of packet delivery ratio.**

Keywords— vehicular ad-hoc networks; position based routing; cross-layer; social aspects; misbehavior;

I. INTRODUCTION

MOBILE Ad Hoc Networks (MANETs) may be defined as distributed wireless communication systems, which comprise potentially a large number of heterogeneous nodes (e.g., PDAs, laptops) belonging to the same or different administrative authorities depending on the specific application domain considered, operating over a large geographical area without existence and support from fixed infrastructure (e.g. base station, access point), under diverse and rapidly changing conditions with respect to connectivity and resource limitations (e.g., bandwidth, energy, memory, computation). These systems are inherently self-organizing and self-configuring so as to cope with dynamic operation conditions.

Vehicular Ad-Hoc Networks (VANETs), one of the successor technologies of MANETs, have in recent years attracted the increasing attention of the researchers, the auto industry and the governments, endeavoring to improve the quality, the safety and the efficiency of future modern transport systems. VANETs are envisioned to form an integral important part of future Intelligent Transport Systems (ITS). Specifically, vehicles will form spontaneous networks, autonomously exchanging important traffic and safety related information in roads and urban environments. VANETs as MANETs are facing diverse and highly changing conditions, constituting, thus, routing protocol design a challenging issue to address for efficient operation in such environments.

Although there are existing routing protocols for MANETs, importing them directly into VANETs, even when amended to fit the vehicular environment, exhibits unsatisfactory performance [1]. Some of the differences that distinguish VANETs from MANETs are the lack of strict energy constraints, the high mobility of the nodes (vehicles), which are however constrained by the road topology, relatively short lived communication links and the characteristics of the communication channel (path loss and fading due to buildings and other vehicles). Amongst topology-based, hierarchical (clustering), flooding (broadcasting) and geographical (position-based) routing protocols, considering the network overhead and or/delay introduced, the complexity of the routing process itself and the inherent dynamic nature of vehicular networks, the last category, i.e., geographical, is the one which best fits vehicular ad-hoc networks.

Geographical routing protocols necessitate each node to know its own position. This could be readily accomplished, assuming that each vehicle is equipped with a GPS device. Apart from GPS, other means of positioning have been

developed and can be used, like triangulation. Besides that, geographical routing protocols assume that every node knows or is able to know the position of the destination when needed. This could be achieved with the use of location services, such as HLS [2]. In a nutshell, geographical routing protocols: a) exhibit improved scalability in large VANETs, since they only use local information to select the next forwarding node, instead of necessitating the knowledge of the complete network graph, as is the case of topology-based protocols, b) introduce less overhead compared to the flooding based protocols, since they only broadcast 1-hop beacon messages, so as to discover neighbors and c) do not incur the clustering overhead compared to hierarchical protocols.

In a similar line of work, ad hoc networks and their related technologies (e.g., VANETs, Opportunistic Networks-OppNets) rely on node cooperation to perform and support basic functions like packet forwarding, routing and network management, a fact that increases network performance sensitivity to nodes' misbehaviour. Misbehaviour, in general, may be defined as deviation from regular functionality, which may be unintentional due to e.g., faults, transmission errors and node mobility or intentional in order for selfish / malicious parties to take advantage of certain situations. Intentional misbehaviour may be attributed to nodes' selfishness, wishing to save their own resources (e.g., CPU, memory, battery) by not forwarding packets that are not directly of interest to them (even though they expect other nodes to forward their own generated traffic) and to nodes' maliciousness that wish to harm and disrupt the normal operation of the network. Depending on the number of misbehaving nodes and their adopted strategies, throughput may be decreased, while network partitioning may result. In any case, nodes' misbehaviour can significantly degrade the performance of the network, which still requires for a high degree of cooperation among its nodes.

Many studies about VANETs were published in the literature in the last decade. The main research activities focused on addressing routing and forwarding issues, since finding end-to-end routing paths in such dynamic environments is regarded as the most challenging issue [3]. On the contrary, trust mechanisms, which are equally important in stimulating cooperation in VANETs, have attracted little to no attention.

On a slightly different note, social network analysis has recently gained a big momentum because of the advent and the increasing popularity of social media, such as blogs, social networking applications, or customer review sites. Social network analysis is the study of social entities (Actors) and their interactions and relationships, which are represented as a graph where each node represents an actor (user) and the edge between two nodes represents their relationship. In this context, actors mostly collaborate with the actors they trust and are influenced by their opinion. Thus, one common type of analysis is the identification of users within certain circles of trust/ distrust (e.g., friends, friends of friends) and the identification of communities of users with similar interests as well the identification of the most "influential" users within [4]. Lately, social-aware networking has attracted the attention of the networking research community, as a field that could further improve various networking operations [5].

Motivated by these demands, this paper investigates the performance of routing protocols in the presence of misbehaving nodes and efficiently enhances Cross-Layer Weighted Position-based Routing (CLWPR), an optimized cross-layer position based routing algorithm for VANETs [6], by incorporating social aspects to its design.

The rest of the paper is organised as follows. In section II we present related work on mechanisms for promoting cooperation in ad-hoc networks, usage of social aspects in the design of routing protocols and the focal characteristics of CLWPR, the adopted position based routing protocol. In section III the proposed protocol (hereafter referred to as *Social CLWPR*) is described in detail and in section IV its performance is compared against the simple CLWPR, assuming the existence of misbehaving nodes. Finally, in section V we conclude our work.

II. RELATED WORK

A. *CLWPR Focal Design Aspects*

The cross-layer, weighted, position-based routing protocol (CLWPR) is a unicast routing protocol specifically designed for VANETs in an urban environment, considering both sparse and dense vehicle traffic. Its basic characteristics are the following. First of all, it is a position based protocol that uses the distance on the road (curvemetric) as a metric instead of the actual geographic (Euclidean) distance. Additionally, it utilizes the prediction of the node's position and navigation information to improve the efficiency of routing protocol in a vehicular network. This allows for more efficient next-hop selection in urban high-build areas, where message dissemination follows the vehicles' travel patterns, decreasing, thus, end-to-end delays. CLWPR also keeps track of link quality, using parameters such as SNIR and MAC frame error rate. Furthermore, nodes' reliability is estimated taking into account the number of consecutive "HELLO" messages received from a particular node. Finally, carry-and-forward mechanism is employed in sparse networks when the node is faced with the local maxima problem (i.e., is found to be the best forwarder to the destination node). To this respect, queuing information is taken into consideration in terms of the number of carry-and-forward packets so as to provide some sort of traffic balancing for better QoS and avoid local maxima.

All this information is jointly combined in a weighting function, that calculates a weight for each neighbouring node, based on which the forwarding selection is performed. CLWPR performance has been comparatively evaluated against relevant position based routing protocols, including GPSR, VADD and GyTAR, by conducting extensive simulation experiments. CLWPR demonstrates higher Packet Delivery Ratio and lower end-to-end delay in urban environments. This is the reason why we have selected CLWPR as the basis of our work and extend it with social information as explained in Section III.

B. Cooperation Enforcement in ad-hoc networking

Recently, the problem of security has received considerable attention by researchers in the ad-hoc networking community. Ad-hoc networks are generally more prone to security threats due to the lack of any pre-established infrastructures, absence of central control, lack of association, sharing of the wireless medium, dynamic topology changes and limited resource availability, whereas attacks from internal nodes are hard to identify and defend [7]. Thus, security establishment in such distributed, open, uncertain, highly dynamic, potentially competitive and resource constrained networks constitutes a difficult task. On the other hand, the success of these systems highly depends on trust mechanisms, building the necessary trust relationships among relevant parties.

In ad-hoc networking, cooperation enforcement schemes provide a "softer" security layer to protect basic networking operations. They fall within two broad categories: trust establishment by means of reputation systems and pricing and credit-based schemes. The first category is based on building reputation of nodes. Reputation mechanisms establish trust by exploiting learning from experience concepts [8] in order to obtain a reliability value (reputation) of system participants in the form of ratings based on past experiences, observations, and other entities' view/opinion. In essence, reputation ratings are seen as a predictor of future behaviour of system participants. In general, reputation systems are considered to sustain rational cooperation and serve as an incentive for good behavior, because good players are rewarded by the society, whereas bad players are penalized. The second category, pricing and credit-based schemes, provide economic incentives for collaboration by charging as well as rewarding service usage and provision (e.g., [9], [10]), either in the form of virtual currency, or service quotas. They require tamper-proof hardware existence or exploitation of trusted third-party services. Additionally, some schemes are inspired from game theory (e.g., [11]).

Even though trust and reputation mechanisms for promoting cooperation is a relatively well-investigated field in a mobile ad-hoc networking setting [12]-[17], this does not stand for OppNets and VANETs, where most of the existing routing protocols assume that all nodes are willing to cooperate. In the context of VANETs, research on trust mechanisms is mostly concerned with determining if and how to trust a specific vehicle or message. To this respect, a few trust models have been proposed for honest information sharing in VANETs (e.g., [18]-[21]). Additionally, trust and reputation mechanisms designed for MANETs cannot be readily applied to VANETs, due to their specific characteristics [20]. Only few research works endeavor to address cooperation in an non cooperative setting (e.g., [22]-[23]). In [22], the authors lay emphasis on cooperation among nodes in vehicular delay tolerant networks, assuming the presence of misbehaving nodes. Two strategies are presented and analyzed, a reputation system and a cooperative watchdog system. The effectiveness of both approaches in improving network performance in the presence of misbehaving nodes is shown. However, focal aspects on their design are not presented in a detailed manner (e.g., how information is represented, how reputation rating information is propagated in the network, how potential inaccurate rating information is handled, if redemption is allowed). In [23], the authors present the proposed SCR protocol, according to which the candidate node for relaying the packet is the one with the higher delivery probability (determined based on the contact frequency between the relay and the destination node, taking also into account an indirect delivery probability that nodes within the contact set of the relay node meet the destination) and the smaller social contribution. In SCR social contribution is defined as the forwarding service that the node provides for other nodes, while a node is permitted to select a relay node with little more social contribution than itself. Thus, social contribution in SCR plays the role of the incentives.

C. Social Aspects in ad-hoc networking

Lately, social-aware routing protocols for ad-hoc networks (mostly in an opportunistic setting) presented in related research literature [24]-[29], exploit social relations among nodes in order to improve the decision taken on the best relay node as well as the best time to forward information to. This is attributed to the observation that people with close relationships (family, friends) sharing similar interests or even belonging within the same community tend to interact more often, more regularly and for longer periods than others, whilst the concept of trust is inherently stronger. In most cases, the next relay node for message transmission is determined on the basis of forwarding capability and trust. Friendship, similarity, community, centrality are some of the social metrics considered when designing message forwarding protocols for opportunistic networks. In a VANET setting, [30] proposes a fuzzy-assisted social-based routing protocol, referred to as FAST, that exploits the social behavior of humans on the road to make optimal and secure routing decisions. Specifically, FAST fuzzy inference system leverages a friendship mechanism to make critical decisions at intersections, assuming that prior global knowledge of real-time vehicular traffic for packet routing from the source to the destination is available. Specifically, real-time information is divided into three classes of mutual relationships (friends, friends-of-friends and non-friends). Based on the number of members of the three classes the node determines which path is more efficient and secure.

As noted in [31], social ties have also been introduced in incentive mechanism design for promoting cooperation in opportunistic networks. Some works utilize social characteristics of nodes in order to determine a composite trust metric and establish trust relations [32], others exploit the notion of community for reputation propagation so as to establish trust in a time efficient manner ([33], [34]), while others consider an initial reputation value based on the social relations of nodes [35].

Social-aware mechanisms in the opportunistic networking context are still in infancy, while several challenges should be efficiently addressed. As noted in [24], a challenging task is how to accurately extract social related information in opportunistic networks due to lack of continuous connectivity and time-varying topology. There are some studies in the context of vehicular networks addressing this aspect. In [36], the authors study mobility in VANETs under a social perspective. Specifically, social metrics (macroscopic and microscopic) are used to characterize vehicles' mobility in realistic datasets; existence of similar behavior and daily patterns in vehicles mobility is found. Moreover, a discussion on how the social metrics may be used to improve the performance of protocols and services is included. A similar work is presented in [37], where the authors present a social analysis of traces that describe features of different groups of vehicles. The acquired results are compared with random graphs so as to increase the validity of the analysis.

Finally, it is noted that combination of multiple social metrics is possible and may lead to performance improvements, even though the decision on which metrics to consider and in which context is not a trivial task. Furthermore, one should carefully consider the trade-off between performance and complexity [24], [25].

III. SOCIAL CLWPR

In this section, we present the key facts and assumptions of our proposed protocol. Social CLWPR is an extension of CLWPR presented in Section II, hence they share some attributes. First, this protocol is designed to be a unicast, multi-hop protocol based o opportunistic forwarding. There is no route discovery before the actual data dissemination; just selection of the next hop on the basis of an objective function that determines / quantifies the "preference" of the node that currently possesses the packet to be forwarded to each neighbouring node and ought to be minimized. The neighbor discovery mechanism is based on 1-hop "HELLO" messages (i.e., beacons) that every node periodically broadcasts. These messages include positioning information (position, velocity, and heading) and other information, according to CLWPR. Additionally, we assume that there is a Location Service that can provide the destination position information.

We hereafter assume the existence of misbehaving nodes that drop incoming packets with a varying probability, depending on whether the received packet originates from a friendly node or not. To this respect an adjacency table, which holds the social relationships of each node, is used to set the preference towards friendly neighbors. Social relationships may be extracted from the online social media the owner of the node (vehicle) is participating, considering different features and attributes, such as explicit user-to-user connections (e.g., friendship, trust or distrust expressions), explicit and implicit user-to-item connections (e.g., comments, like and dislike statements), taking into account the multitude of user-provided tags, inherent connectivity between users and their posted items and high update rate [38]. Taking into account that the notion of trust is bound to the permanent link between two users in a social network (e.g., the blogroll list of a user in the case of blogs, the "friend" links in the case of social networking applications or the links to the "members of trust" in the case of consumer networks), in the current study we limit our attention to this metric, attributing a high level of trust and cooperation to nodes with whom there is a close/ friendly relationship and a low level of trust and cooperation to nodes with whom there exists a distrust relationship, as indicated in the social media.

Objective Function

As Social CLWPR is an opportunistic protocol, the preference value towards each neighbouring node is calculated each time a node possesses a packet to be sent or forwarded towards a destination node. Thus, for each unique destination address that a node has to send a packet, it calculates the preference value of every node in its neighbouring list towards that destination (including itself) using eq.(1). For a specific destination, the node with the minimum estimated preference value is selected as the next hop forwarder. In case of local maxima, i.e. the current node has the least preference value, as already mentioned, carry-and-forward mechanism is employed until a suitable next-hop is identified.

At this point it should be stressed that we only use localised information to select the forwarding node and don't need to know the complete network topology or a specific route to the destination. Furthermore, if a node does not have a packet to send/forward then it does not need to calculate a routing table and, thus, the computations are minimized.

$$\begin{aligned} Objective\ Function = \\ w_1 * NormDistance + w_2 * NormAngle \\ + w_3 * NormRoad + w_4 * NodeReliability \\ + w_5 * MAC_{info} + w_6 * CNF_{info} \\ + w_7 * WeightedSNIR + w_8 * SocialRelation \end{aligned} \quad (1)$$

where

NormDistance represents the normalized curvemetric distance between two nodes over a reference communication range. It takes into account the predicted location of the second node using velocity and heading information provided in the "HELLO" messages.

NormAngle represents the mutual direction of the two nodes, if they approach each other or moving apart. This is quantified with the cosine of the angle θ between the velocity vectors of the two nodes (eq. (2)).

$$NormAngle = \cos(\theta) \quad (2)$$

NormRoad takes value 0 if the two nodes move on the same road, or 1 if the nodes travel on different roads (eq. (3)).

$$NormRoad = \begin{cases} 0 & if\ vehicles\ on\ same\ road \\ 1 & if\ vehicles\ on\ different\ roads \end{cases} \quad (3)$$

As mentioned earlier, *NodeReliability* is calculated based on the number of consecutive received "HELLO" messages according to certain thresholds (eq. (4)). These can be varied depending on the "HELLO" emission rate.

$$NodeReliability = \begin{cases} 1, if\ Hello\ Count\ \leq 2 \\ 0.5, if\ 2\ < Hello\ Count\ \leq 4 \\ 0, if\ Hello\ Count\ > 4 \end{cases} \quad (4)$$

MACinfo represents the level of contention in the area close to the neighbour node and accounts for the average number of collisions during the period between two "HELLO" messages.

CNFinfo indicates the level of utilization of the node in terms of number of cached packets and is used in order to penalize nodes that are found in local maximum condition.

WeightedSNIR represents the quality of the channel between the two nodes, giving preference to nodes far away from the sending node, but not very close to the edge where the drop probability may be high. Thus, higher preference value is attributed to nodes with lower SNIR. In eq. (5), variables *a, b* are optimization parameters and the range to which the preference is given, is determined by the threshold *SNIRth.*

$$WeightedSNIR = \begin{cases} ax^2, if\ SNIR \leq SNIR_{th} \\ be^{-x}, if\ SNIR \geq SNIR_{th} \end{cases} \quad (5)$$

SocialRelation indicates the social relationships between two nodes, with -1 representing a friendly / trustworthy relation, 1 an unfavourable / untrustworthy one and zero is taken for neutral relations or for nodes with none existing relation. The relationships are obtained from the adjacency matrix.

$$SocialRelation = \begin{cases} -1\ for\ trusted\ connections \\ 0\ for\ neutral\ relations \\ 1\ for\ distrusted\ connections \end{cases} \quad (6)$$

Weights w_i ,$i \in [1,8]$ provide the relative significance of the eight factors to the preference value calculation in order to make an efficient forwarding decision.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed protocol and provide indicative evidence of its efficiency against the simple CLWPR protocol, incorporating various degrees of nodes' misbehavior. The performance metric considered is the packet delivery ratio (PDR). The simulation experiments were carried out using the NS3 simulator [39].

We consider an area of 2000x2000 meters, employing a 5x5 Manhattan Grid road network as shown in Fig. 1, where horizontal and vertical streets are divided into two lanes. In vertical streets, nodes can move in north and south direction and in horizontal streets nodes can move in east and west direction. 200 vehicle nodes are moving in the considered area with a speed of 10 m/sec. The movements of nodes are generated using mobility generator tool Bonnmotion [40]. There are 10 source/sink data pairs sending UDP data at an application rate of 2.048 Kb/s. The communication range is set to be 500 meters according to the IEEE802.11p standard [41]. The simulation environment details are shown in TABLE I.

In the first set of experiments we assume an increasing percentage of misbehaving nodes in the network that drop received packets with varying probabilities (i.e., *p=0.3, p= 0.6* and *p=0.9*). In case a social relationship between two nodes exists (as indicated by the adjacency matrix), nodes which are explicitly connected with a trust / friendship link exhibit low probability to drop their packets (i.e., *p=0.1*), while on the other hand, nodes with an explicit distrust connection tend to drop their packets with high probability (i.e., *p=0.9*). Each simulation experiments lasts for 200 simulated seconds, while several runs per experiment have been performed (10 runs), providing in the following figures the mean values extracted.

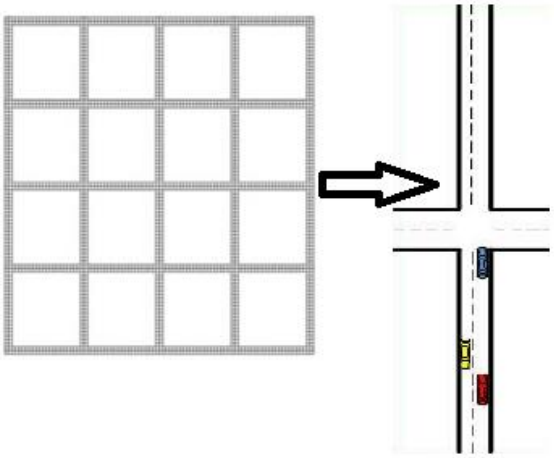

Figure 1: 5x5 Manhattan Grid Road Network

TABLE I
SIMULATION PARAMETERS

Mobility model	Manhattan Grid Model
Simulation duration	200 seconds
Simulation area	2000x2000 meters
Number of nodes	200
Node speed	10m/s
Sink data pairs	10
UDP data rate	2048Kb/s
WiFi	6Mb/s (802.11p)

Fig.2 depicts the packet delivery ratio succeeded by CLWPR and SocialCLWPR, respectively. As it may be observed, the PDR decreases as the percentage of misbehaving nodes increases in the network. Additionally, the SocialCLWPR outperforms CLWPR in all cases (by 30 % maximum).

In the following set of experiments, we consider an increasing percentage of misbehaving nodes in the network (30%, 60% and 90%) that drop received packets with an increasing probability. Fig. 3 graphically illustrates the obtained results. The PDR decreases as the packet drop probability of misbehaving nodes increases.

In the previous experiments we assumed that the number of trusted connections was the same. Fig. 4 depicts the packet delivery ratio for different values (20, 50, 100) of trusted connections. It is obvious that the PDR increases as the total number of trusted connections increases.

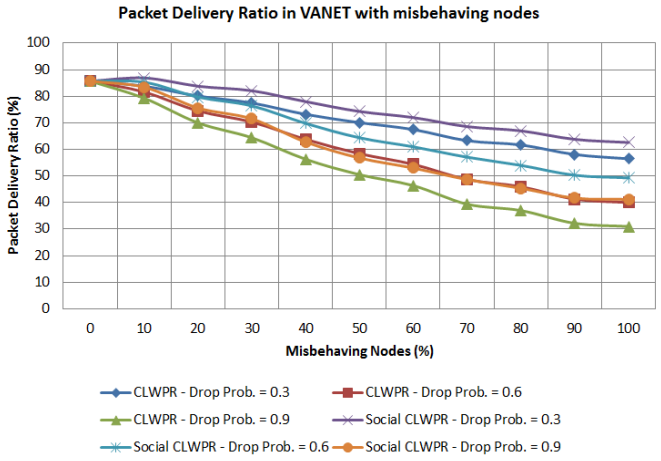

Figure 2: PDR in VANETS with misbehaving nodes

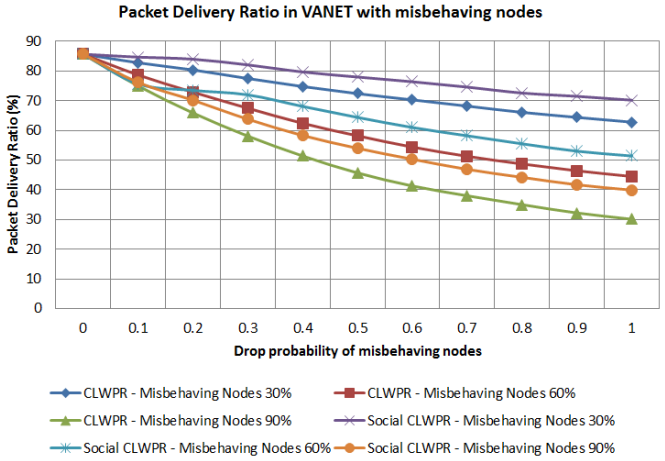

Figure 3: PDR in VANETS with misbehaving nodes

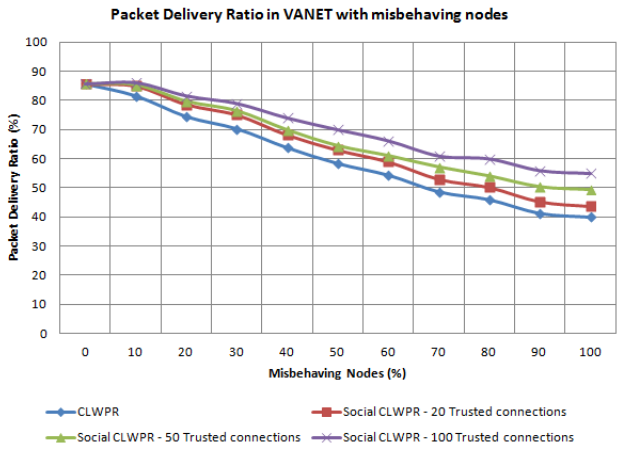

Figure 4: PDR in VANETS with different trusted connections

V. CONCLUSIONS

In this paper, the authors present Social CLWPR, a socially enhanced position-based routing protocol for efficiently handling misbehavior in urban VANET environments. Specifically, assuming the presence of selfish/malicious nodes that intentionally drop packets, Social CLWPR enhances CLWPR by introducing social aspects to its design, favoring on the decision on next hop forwarders nodes with whom an explicit trusted /friendly social connection exists. Social CLWPR performance is comparatively evaluated against CLWPR and initial results acquired demonstrate improved performance in terms of packet delivery ratio (improvement by 30%). Concerning future work, we intend to employ a reputation based mechanism in order to estimate the packet drop probability of nodes, even in case social relationships exist, and take these values into account when deciding on the next forwarding nodes, with the social relationship information forming the initial reputation of nodes.

REFERENCES

[1] V. Timcenko, M. Stojanovic, and S. B. Rakas, "MANET routing protocols vs mobility models: performance analysis and comparison", in Proc. of the *International Conference on Applied Informatics and Commuinications*, pp. 271-276, 2009.

[2] W. Kieβ, "Hierarchical location service for mobile ad-hoc networks", Master Thesis, University of Mannheim, 2003.

[3]

[4] Iraklis Varlamis, Magdalini Eirinaki, Malamati Louta, "Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations", Springer Series on "Lecture notes in Social Networks", Tansel Ozyer et al. (eds.): "The influence of Technology on Social Network Analysis and Mining", No. 6, DOI 10.1007/978-3-7091-1346-2__3.

[5] Feng Xia, Li Liu, Jie Li, Jianhua Ma, Athanasios V. Vasilakos, "Socially Aware Networking: A Survey", *IEEE Systems Journal*, Vol. 9, Issue 3, pp. 904-921, 2013.

[6] Konstantinos Katsaros, Mehrdad Dianati, Rahim Tafazolli and Ralf Kernchen, "CLWPR – A Novel Cross-Layer Optimized Position Based Routing Protocol for VANETs", in Proc. of the *2011 IEEE Vehicular Networking Conference*, pp. 139-146, 2011.

[7] Deng, H., Li, W., Agrawal, D. P., "Routing security in wireless ad hoc networks", *IEEE Communications Magazine*, Vol. 40, pp. 70-75, 2002.

[8] Sutton, R. S., Barto, A. G. Reinforcement learning: An introduction (Adaptive computation and machine learning), MIT Press, 1998.

[9] Buttyán, L., Hubaux, J.-P., "Stimulating cooperation in self-organizing mobile ad hoc networks", *ACM Journal for Mobile Networks, special issue on Mobile Ad Hoc Networks*, Vol. 8, Issue 5, pp. 579-592, 2003.

[10] Zhong, S., Chen, J., Yang, Y. R., "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks", in Proc. of *IEEE INFOCOM'03*, San Francisco, USA, 2003.

[11] Raya, M., Shokri, R., Hubaux, J.-P., "On the tradeoff between trust and privacy in wireless ad hoc networks", in *ACM WiSec Conference*, pp. 75-80, 2010.

[12] Marti, S., Giuli, T. J., Lai, K., Baker, M., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", *in ACM International Conference on Mobile Computing and Networking Conference (MobiCom)*, 2000.

[13] Buchegger, S. Le Boudec J.-Y., "Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad hoc networks)", in *MobiHoc'02, IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2002.

[14] Michiardi, P., Molva, R., "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks", in *CMS'02 Communications and Multimedia Security Conference*, 2002.

[15] He, Q., Wu, D., Khosla, P., "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks", in *WCNC'04 IEEE Wireless Communications and Networking Conference*, 2004.

[16] Bansal, S., Baker, M., "Observation-based Cooperation Enforcement in Ad hoc Networks", Technical Report, Stanford University, 2003.

[17] Hu, J., Burmester, M., "LARS: a locally aware reputation system for mobile ad-hoc networks", in *44th annual ACM Southeast Regional Conference*, 2006.

[18] F. Dotzer, L. Fischer, and P. Magiera, "VARS: A Vehicle Ad-hoc network Reputation System", in *sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05)*, pp. 454-456, 2005.

[19] Nai-Wei, L., Hsiao-Chien, T., "A reputation system for traffic safety event on vehicular ad hoc networks" in *EURASIP Journal on Wireless Communications and Networking*, 2009.

[20] Huang, Z., Ruj, S., Cavenaghi, M.A. et al., "A social network approach to trust management in VANETs", in *Peer-to-Peer Netw*., Vol. 7, Issue 3, pp 229–242, 2014.

[21] Chen, C., Cohen, R., Zhang, J, "A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks", in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 1, Issue 3, pp. 3-15, 2010.

[22] Joao A. F. F. Dias, Joel J. P. C. Rodrigues, Neeraj Kumar, Kashif Saleem, "Cooperation strategies for vehicular delay-tolerant networks", in *IEEE Communications Magazine*, Vol. 53, Issue 12, pp. 88-94, 2015.

[23] H. Gong, L. Yu, and X. Zhang, "Social contribution-based routing protocol for vehicular network with selfish nodes", *International Journal of Distributed Sensor Networks*, Vol. 2014, pp. 1-12, 2014.

[24] Zhu, Y., Xu, B., Shi, X., Wang, Y., "A survey of social-based routing in delay tolerant networks: positive and negative social effects", *IEEE Communications Surveys & Tutorials*, Vol. 15, Issue 1, pp. 387–401, 2013.

[25] K. Wei, X. Liang, K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: Applications taxonomy and design-related issues", *IEEE Communications Surveys & Tutorials*, Vol. 16, Issue 1, pp. 556-578, 2014.

[26] W. Moreira, P. Mendes, "Social-aware Opportunistic Routing: The New Trend", in: *I. Woungang, S. Dhurandher, A. Anpalagan, A. V. Vasilakos (Eds.), Routing in Opportunistic Networks*, Springer Verlag, 2013.

[27] Katsaros D., Dimokas N., Tassiulas L., "Social network analysis concepts in the design of wireless ad hoc network protocols", *Network IEEE*, Vol. 24, Issue 6, pp. 23-29, 2010.

[28] Papadimitriou A., Katsaros D., Manolopoulos Y., "Social Network Analysis and Its Applications in Wireless Sensor and Vehicular Networks", In: *Sideridis A.B., Patrikakis C.Z. (eds) Next Generation Society. Technological and Legal Issues. e-Democracy 2009*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 26, Springer, Berlin, Heidelberg, 2010.

[29] Yanru Z., Lingyang S., Chunxiao J., et al, "A Social-Aware Framework for Efficient Information Dissemination in Wireless Ad Hoc Networks-Ad Hoc and Sensor Networks", *IEEE Communications Magazine*, Vol. 55, Issue 1, pp. 174-179, 2017.

[30] Khokhar, R.H., Md Noor, R., Ghafoor, K.Z. et al., "Fuzzy-assisted social-based routing for urban vehicular environments", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2011, Issue. 1, pp. 178, 2011.

[31] Nikolaos Mantas, Malamati Louta, Eirini Karapistoli, Georgios Karetsos, Stylianos Kraounakis and Mohammad S. Obaidat, "Towards and Incentive – Compatible, Reputation-Based Framework for Stimulating Cooperation in Opportunistic Networks: A Survey", submitted for publication to *IET Networks journal*.

[32] L. Yao, Y. Man, Z. Huang et al., "Secure Routing based on Social Similarity in Opportunistic Networks", *IEEE Transactions on Wireless Communications*, Vol. 15, Issue 1, pp. 594-605, 2016.

[33] Wei, L.F.; Zhu, H.J.; Cao, Z.F.; Shen, X.M., "SUCCESS: A secure user-centric and social-aware reputation based incentive scheme for DTNs", *Ad Hoc & Sensor Wireless Networks*, Vol. 19, Issue 1-2, pp. 95–118, 2013.

[34] Wei L., Zhu H., Cao Z., Shen X., "MobiID: A User-Centric and Social-Aware Reputation Based Incentive Scheme for Delay/Disruption Tolerant Networks", In: *Frey H., Li X., Ruehrup S. (eds) Ad-hoc, Mobile, and Wireless Networks. ADHOC-NOW 2011*, Lecture Notes in Computer Science, Vol 6811. Springer, Berlin, Heidelberg, 2011.

[35] Radu-Ioan Ciobanu, Radu-Corneliu Marin, Ciprian Dobre, Valentin Cristea, "Trust and reputation management for opportunistic dissemination", *Pervasive and Mobile Computing*, Vol. 36, pp. 44-56, 2017.

[36] F. Cunha, A. Carneiro Viana, R. A. F. Mini, and A. A.F. Loureiro, "How effective is to look at a vehicular network under a social perception?", in *1st International Workshop on Internet of Things Communications and Technologies (IoT'13) (IoT'2013)*, Lyon, France, 2013.

[37] F. D. Cunha, A. Carneiro Vianna, R. Mini, A. Loureiro et al., "Is it possible to find social properties in vehicular networks?", *Computers and Communication (ISCC) 2014 IEEE Symposium*, pp. 1-6, 2014.

[38] Magdalini Eirinaki, Malamati Louta, Iraklis Varlamis, "A Trust-Aware System for Personalized User Recommendations in Social Networks", *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 44, Issue 4, pp. 409– 421, 2014.

[39] "The NS-3 network simulator." Available online. http://www.nsnam.org

[40] Bonn Motion, http://net.cs.unibonn.de/wg/cs/applications/bonnmotion/

[41] "IEEE Standard for Information technology–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6:Wireless Access in Vehicular Environments," 2010.