International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.10, pp : 1049-1055 1 Oct. 2013

Design Approach for Cooperative Security in Vehicular Communication Systems

Pravin P. Ashtankar, Sonali N. Dhurvey
[1]PCE, Nagpur. [2]PIET, Nagpur

Abstract—A Vehicular Ad-Hoc Network (VANET) is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed roadside equipment. The key operation in VANETs is the broadcast of messages. Its main goal is to improve safety and comfort for passengers, but it can also be used for commercial applications. In this latter case, it will be necessary to motivate drivers to coop-erate and contribute to packet forwarding in Vehicle-to-Vehicle and Vehicle-to-Roadside communications. This paper examines the problem, analyzes the drawbacks of known schemes and proposes a new secure incentive scheme to stimulate cooperation in VANETs, taking into account factors such as time and distance.

Keywords. Cooperative security, Vehicular Ad-Hoc Network, VANET

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are important compo-nents of Intelligent Transportation Systems. The main benefit of VANET communication is seen in active safety systems that increase passenger safety by exchanging warning messages between vehicles. Other promising commercial applications are Added-Value Services such as: advertising support [6], request/provide information about nearby companies, access to Internet, etc.

A VANET may be seen as a special type of ad-hoc network used to provide communications between On-Board Units (OBUs) in nearby vehicles, and between OBUs in vehicles and Road-Side Units (RSUs), which are fixed equipment located on the road. In particular, this paper deals with the topic of Inter-Vehicle Communication when the systems in a VANET do not rely on RSUs, and consequently constitute a Mobile Ad-hoc Network (MANET).

The main advantage of VANETs is that they do not need an expensive infrastructure. However, their major drawback is the comparatively complex networking management system and security protocols that are required. This difficulty is mainly due to some specific characteristics of VANETs that allow differentiating them from the rest of MANETs such as their hybrid architecture, high mobility, dynamic topology, scalability problems, and intermittent and unpredictable com-munications. Consequently, these features have to be taken into account when designing any management service or security protocol.

In order to bring VANETs to their full potential, appropri-ate schemes to stimulate cooperation need to be developed according to the specific properties and potential applications of VANETs. Many incentive schemes to stimulate cooperation in ad-hoc networks may be found in the bibliography [5] [9] [10] [11]. Some authors have made first approaches to the topic of cooperation in VANETs [3] [4] [12] [13]. Related to the proposal here described, Buttyan and Hubaux proposed in [1] and [2] the use of virtual credit in incentive schemes to stimulate packet forwarding. Also, Li et al. discussed some unique characteristics of the incentive schemes for VANETs in [7] and proposed a receipt counting reward scheme that focuses on the incentive for spraying. However, the receipt counting scheme proposed there has a serious overspending problem. Based on the specific characteristics of VANETs, a more comprehensive weighted rewarding method is proposed here.

In particular, the proposed scheme is based on incentives where the behavior of a node is rewarded depending on its level of involvement in the routing process. Schemes based on reputation were here discarded due to the high mobility of nodes in VANETs, which makes infeasible to maintain historical information about peers behavior.

Note that an important problem that must be dealt with in rewarding incentive schemes is the possibility for selfish or malicious users in the vehicles to exaggerate their contribution in order to get more rewards. In our proposal, we assign different possible incentives to vehicles according to their con-tribution in packet forwarding, in an effort to achieve fairness and provide stimulation for participation. Our scheme utilizes a weighted rewarding component to decide the specific incentive in each case so they help to keep the packet forwarding attractive to the potential intermediate vehicles.

The rest of the paper is organized as follows. Section II gives an overview of the security mechanisms developed for vehicular communication systems. Section III underlines the drawbacks of the existing reputation-based and credit-based systems. The proposed security scheme is introduced in Sec-tion IV. An group-based authentication scheme is proposed in Section V.

Section VI discusses the results of the experiments we have conducted. Finally, Section VII concludes the paper and gives some insights on the potential extensions.

II. OVERVIEW ON THE SECURITY VEHICULAR COMMUNICATION SYSTEMS

Vehicular systems have many characteristics that make them different from the traditional mobile systems and computer networks connected to the Internet. These networks are characterized by high mobility of the nodes and rapidly changingtopologies. Vehicular applications are generally divided into two categories. The first category includes applications that relate to security and ergonomy of the driving process. The main purpose of these applications is to reduce the number of traffic accidents and to solve the congestion problems on roads and highways. The second category focuses on ensuring comfort for the driver and the passengers while travelling. For example, access to information and recreational (ie. Internet, music, films ...), the payment of fees and costs of highways, parking, and possibly, fines.

In the near future, VANETs will combine a variety of wireless technologies like DSR (Dedicated Short Range) communications described in the draft of standard for VANETs IEEE 802.11p WAVE (Wireless for Access Vehicular Environments), with Cellular, Satellite and WiMax technologies. Therefore, it is expected that each vehicle will have as part of its equipment: a black box (EDR, Event Data Recorder), a registered identity (ELP, Electronic License Plate), a receiver of a Global Navigation Satellite System like GPS (Global Positioning System) or Galileo, sensors to detect obstacles at a distance lesser than 200 ms, and some special device that provides it with connectivity to an ad hoc network formed by the vehicles. Such a device allows the node to receive and send messages through the network.

Two hypotheses that are necessary to guarantee the security of VANETs are that these devices are reliable and tamper-proof, and that the information received through sensors is also trustworthy. It is generally assumed that the messages sent through the VANET may be digitally signed by the sender with a public-key certificate. This certificate is generally emitted by a Certification Authority (CA) that is admitted as reliable by the whole network. The moments corresponding to vehicle purchase and to the periodic technical inspections might be respectively associated to the emission and renovation of its public-key certificate.

Note that the use of PKIs in VANETs implies the problem of the enormous cost of the management of a giant CA, with the corresponding high consumption of resources. Furthermore, it makes it very difficult to deal with anonymity. Since public keys should be frequently updated in order to protect privacy, it becomes impractical that all vehicles store the public keys of the remaining nodes. Consequently, proposals such as self-organized and distributed certification of public keys might be good solutions. Note that any of these proposals must be combined with a cooperation enforcement mechanism between nodes.

III. SHORTCOMINGS OF THE EXISTING APPROACHES

A VANET may be seen as a variation of a MANET where the nodes are vehicles. In both types of networks, cooperation between nodes is required for the adequate performance, so there might be thought that cooperation tools for MANETs can be also used for VANETs. In MANETs we can find two main approaches: Reputation-based schemes where packets are forwarded through the most reliable nodes, and Credit-based schemes where packet-forwarding is dealt with as a service that can be evaluated and charged. In our work we have analyzed both schemes in order to find out whether they are suitable for VANETs.

A. Shortcomings of reputation-based systems

An important characteristic of VANETs is the high mobility of nodes. Taking into account such a parameter, it is impossible to establish a reputation-based scheme because it is infeasible to maintain historical information about peers' behavior in a VANET. This is because it is possible that two vehicles meet just once in a long period of time, and it is very difficult to listen whether a neighbor node actually forwards a packet.

B. Shortcomings of credit-based systems

Incentive schemes have been proposed in order to solve cooperation problems in MANETs. The so-called Packet Purse Model where every source node puts a sum of money that it considers enough to reach the destination has an overspending problem because the source vehicle can not predict accurately the global size of the required reward. Other known model is the so-called Packet Trade Model where the destination node pays the reward. In this case the model has problems because source nodes can send all the packets they want as they have not to pay for them. This model produces a network overload. Consequently, we can conclude that none of both schemes are a good solution for MANETs or for VANETs.

IV. PROPOSED COOPERATIVE SECURITY SCHEME

A typical packet forwarding process in VANETs where the important features of routing in VANETs can be globally represented by the following steps:

1) The root node corresponds to the source vehicle that first sprays the message.

2) Each intermediate vehicle corresponds to one node in the tree.
3) Each node ignores those packets that it had previously received. Consequently, every vehicle is present just once in every forwarding tree.

4) Each link in the tree corresponds to an encounter in the vehicular network, which is associated with a timestamp and the spatial coordinates indicating the position of the vehicles.

According to the store-and-carry paradigm [7] [8], if an intermediate vehicle stores a packet for a long time or actively sprays the packet to other vehicles, the packet will be either more likely to reach the intended destination, or to arrive to more destinations, depending on the specific goal of the routing. Therefore, by simply combining storage time and number of sprays, we can define a useful contribution metric for the intermediate vehicles. In order to stimulate intermediate vehicles to contribute more, the source vehicle should reward each intermediate vehicle according to its contribution.

Initially, the contribution C_i to packet forwarding of a node i during the forwarding process may be modeled as a linear convex combination balancing numbers of forwarding f_i and the period the packet is stored t_i:$C_i = t_i + (1)f_i$.

However, this basic model implies a constant share reward R which is promised for the source node to each intermediate node. This model may cause an overspending problem because the source vehicle cannot guess in advance the total reward since the number of nodes in the tree cannot be predicted easily. Such a problem might be solved maintaining constant the total reward and calculating the reward associated to each intermediate node R_i after the packet reaches the destination according to the following formula:

$R_i = \frac{R\,C_i}{C}$ where $C = \sum_{i} C_i$

When the packet reaches the destination, each node i that participated in the forwarding should report its contribution C_i to the source. The final contribution C is calculated through the sum of the partial contribution of each node in the forwarding tree. Each intermediate node will receive R_i as reward for forwarding. This model cannot be considered neither a good solution because selfish nodes might prefer keeping the packet rather than retransmitting it since they do not know in advance how much they can earn for forwarding and/or they might prefer not to share the reward. It happens when an intermediate node forwards the packet to a non final node because its proportional reward might decrease.

In our first proposal we incorporate several parameters to be considered when dealing with rewarding. They are related to information such as packet delivery deadline and number of forwardings. In order to avoid that nodes prefer keeping the packet rather than retransmitting it, we consider that a packet should have a deadline depending on the characteristics of the information contained. If the sent information is added-value information, then the deadline will be longer, whilst if the information is related to traffic safety, the deadline must be very short due to the urgency of transferring the information. The following notation is used to describe the parameters for the computation of rewards:

Packet delivery deadline T_j.

Period t_{ij} that packet j is stored by node i.

Number of forwardings f_{ij} of packet j by node i before the deadline T_j.

Balancing factor

With these parameters we present our first proposal of contribution function: $C_{ij} = (t_{ij}T_j) + (1)f_{ij}$ where

2 (0; 1):

In this first approach to the solution, the contribution of node i for spreading packet j is proportional to the time t_{ij} the packet is transported by the packet deadline T_j, and to the number of the forwardings f_{ij}. By counting the number of forwardings in this function, the objective is to encourage nodes to forward packets and not to keep them without forwarding them.

If the rate between time and deadline $t_{ij}=T_j$ were consid-ered as factor, when the message is urgent and the deadline is short, the contribution would be higher. However in such a case, once the time t_{ij} overpasses the deadline T_j, the contribution still goes on increasing and even faster because the proportional factor is greater than 1. This effect can be corrected by using the inverse of the deadline so that the more urgent the message, the greater the value $1=T_j$. Therefore, when the time that the packet is stored passes the deadline the user contribution is no more increased. However, this is neither a good solution because although the deadline has been reached, the forwarding node continues getting a reward although it is a small amount.

Our second proposal tries to solve these problems. We propose a new contribution function in which three parameters are used, which can be interesting both for the source node and/or for the forwarding node. In particular we consider the following additional notation to describe the parameters for the computation of rewards:

Distance d_{ij} between source and destination nodes when the

packet j is relayed by node i.

Maximum distance D_j where the information in the packet j is considered interesting by the receivers.

Each of the parameters considered in this convex function has a balancing factor, represented by $_1$, $_2$ and $_3$. The value that is assigned to each $_i$ depends on the relevance that the source node prefers to assign to each component represented in the contribution function:

$$C_{ij} = {}_1 T_j(1 \ e^{\ tij}) + {}_2 f_{ij} + {}_3 (D_j(1 \ e^{\ dij}) + D_j)$$

$$\sum_{k=1}^{3} {}_k = 1:$$

In the next subsections each part of this function is detailed, and both the justification why they are used and the repercus-sion they have in the contribution function are given.

A. Time

As discussed above, time is one of the most important parameters when trying to assure that a packet reaches the intended destination. If a vehicle stores a packet for a long time, it could forward the package to more vehicles. However, this parameter could produce a selfish behavior because a node could prefer not to forward it and in this way not to share the final reward with potential forwarding nodes. This effect is avoided by considering in the proposed metric the component associated to the following formula:

$$T_j(1 \ e^{\ tij}).$$

This function corresponds to the Stokes formula, which has a characteristic asymptotical behavior. This function is intended to set a maximum time T_j that a node should store one packet. Note that the value of contribution increases when time increases. When t_{ij} reaches the threshold T_j, the growth of contribution stops. In this way, a selfish behavior can be avoided because if the time threshold is properly set, those vehicles that retransmit the packet before the deadline will have increased their contribution.

Note in the example of Figure 1 that the value of contri-bution increases when the time increases, and that when t_{ij} reaches the threshold T_j the contribution increase stops. In this way, both selfish behavior and forwarding after deadline are discouraged because vehicles that retransmit the packet before deadline will have their contribution increased.

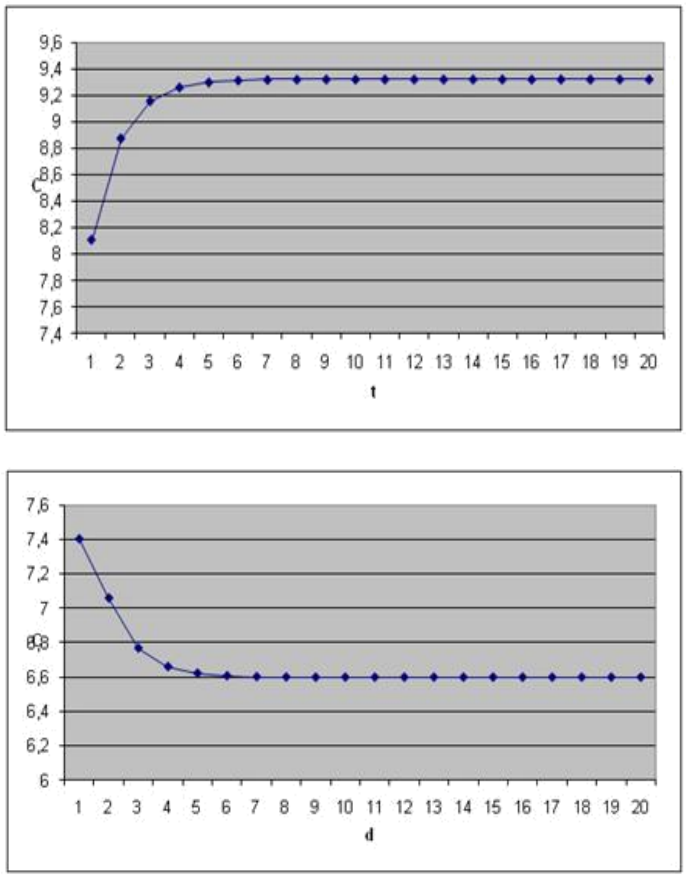

Fig. 1. Contribution versus time and distance

B. Forwarding

The second term in the proposed contribution metric is related to the ultimate goal of our work. It deals with measuring the forwarding of packets by each intermediate node. This process is quite simple. It has not any restriction such as maximum or minimum possible values. It consists of increasing the contribution of node i to relay the packet j by:

f_{ij}.

According to this factor, the more the vehicles collaborate in forwarding a packet, the bigger their final contribution is. In the proposed function, this parameter is the one that increases the contribution faster before the deadline. Consequently, the balancing factor $_2$ must be higher than the other two factors in order to encourage the forwarding of packets.

C. Distance

The evaluation of the effect of distance in the share reward-ing process is the goal of the third term of the contribution function.

This term has been incorporated thinking that in many cases information generated at a certain location is not interesting out of a radius distance from than point. With this idea in mind, when the vehicles go too far from the source of the original packet, this value decreases.

For example, if we talk about an accident in a city center, it has not sense that the message reaches a neighbor city. Other possible situations where the same idea is applicable is where the information is sent by a commercial centre, hotel or restaurant, for instance.

This term is similar to the one related to time commented in subsection IV-A. The goal is to obtain a function with asymptotical behavior that tends to zero when distance is near to D_j. The value D_j is established by the source node. The

expression that models this behavior is:
$D_j(1 \quad e^{dij}) + D_j$.
Figure 1 shows an example where as the vehicle moves away from the source its contribution decreases, and when it reaches certain point it nulls. In this way, the vehicle does not get any benefit if it retransmits the packet outside the radio.

V. GROUP-BASED AUTHENTICATION IN VANETS

In this paper group formation is proposed as a valid strategy to strengthen privacy and provide authentication, while reduc-ing communications in VANETs. In particular, we propose location-based group formation according to dynamic cells dependent on the characteristics of the road, and especially on the average speed. In this way, any vehicle that circulates at such a speed will belong to the same group within its trajectory. We also propose here that the leader of each group be the vehicle that has belonged to the same group for the longest time.

According to our proposal, V2V between groups will imply package routing from the receiving vehicle towards the leader of the receiving group, who is in charge of broadcasting it to the whole group if necessary. If the cells have a radio that is greater than the wireless coverage of the OBU, the group communication may be carried out by proactive Optimized Link State Routing (OLSR).

In the two phases corresponding to group formation and node joining, each new node has to authenticate itself to the leader through asymmetric authentication. Later, the leader sends a shared secret key to it, encrypted with the public key of the new node. In particular, this secret key is shared among all the members of the group, and used both for V2V within the group and for V2V between groups, as it is explained in the following sections.

Unlike I2V communication, in V2I communications privacy is an essential ingredient. Here we propose a challenge-response authentication protocol based on a secret-key ap-proach where each valid user is assigned a random key-ring with k keys drawn without replacement from a central key pool of n keys.

during authentication each user chooses at random a subset with c keys from its key-ring, and uses them in a challenge-response scheme to authenticate itself to the RSU in order to establish a session key, which is sent encrypted under the RSU's public key.

This scheme preserves user privacy due to the feature that each symmetric key is with a high probability (related to the birthday paradox and dependent on the specific choice of parameters) shared by several vehicles.

When a vehicle wants to communicate with the RSU, it sends an authentication request together with a set of c keys taken at random from its key-ring and a timestamp. All this information is then encrypted by the established session key. Note that a set of keys, instead of only one key, is proposed for authentication, because there is a high probability for the OBU to have one key shared by a large amount of vehicles. This makes it difficult to identify a possible malicious vehicle if just one key is used. However, there is a much lower probability that a set of a keys be shared by a large number of vehicles, and so it is much easier to catch a malicious vehicle in the proposal.

After the RSU gets the authentication request from the vehicle, it creates a challenge message by encrypting a random secret with the set of keys indicated in the request, by using Cipher-Block Chaining (CBC) mode. Upon receiving the challenge, the vehicle decrypts the challenge with the chosen keys and creates a response by encrypting the random secret with the session key. Finally, the RSU verifies the response and accepts the session key for the next communications with the vehicle.

In the first step, in order to make easier the task of checking the key subset indicated in the request by the RSU, we propose a tree-based version where the central key pool of n keys may be represented by a tree with c levels. Each user is associated to k=c leaves, and each edge represents a secret key.

In this way, the key-ring of each user is formed by several paths from the root to the leaves linked to it. During each authentication process the user chooses at random one of its paths, which may be shared by several users. In this way, to check the keys, the RSU has to determine which first-level key was used, then, it continues by determining which second-level key was used but by searching only through those second-level keys below the identified first-level key. This process continues until all c keys are identified, what at the end implies a positive and anonymous verification. The key point of this proposal is

that it implies that the RSU reduces considerably the search space each time a vehicle is authenticated.

VI. SIMULATION ANALYSIS

In order to make a study of the proposal, several VANETs simulations have been implemented in Matlab. The simulation parameters are the following: 15 nodes placed at random in an area of 800m x 800m. The range of action of each node is 100m. In each simulation, a node is randomly chosen and it starts sending a packet to its neigbours, who send it to all the nodes they meet inside their range of action. In Figure 2 we analyze the relationship among the rewards and the different parameters of the contribution function. According to the time plot, the scheme seems to send bigger rewards to those nodes who store packets for longer. However, note that these rewards are influenced by the number of forwards and the distance between the source node and the nodes forwarding the packet. In the forwards graph, the reward average increases according to the number of forwards. Finally, in the distance plot the scheme seems to give lower rewards to those nodes whose distance increases according to the source node initial position. For some nodes at a large distance, the reward average increased due to that their spray was bigger than the spray of the nodes in the same distance. This scheme provides more reward to the nodes that effectively forwarded the packet
for a long time. In fact, the results of our experiments shows that the proposed scheme is characterized by a better fairness than the existing schemes. Also according to Figure 3, the proposal gives more reward to those nodes with higher contri-butions, which are usually those nodes that have more children. Consequently, cooperation among nodes is guaranteed thanks to the proposal.

VII. CONCLUSION

In this paper we have seen that a simple adaptation of known cooperation enforcement schemes defined originally for MANETs is not adequate to incentivize cooperation in VANETs. Consequently, we have proposed a new scheme where incentives are defined by a convex function that de-pends on different parameters. We have designed a metric for contribution according to the characteristics of VANETs and to parameters that are important both for source node and for enforcing cooperation among nodes. We conclude from our study that when designing these methods for distributing a reward, the parameters to be taken into account should be carefully assessed according to the network conditions.

REFERENCES

i. *Buttyan, L. and Hubaux, J.P.: Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. ACM Mobile Networks and Applications, 8(5), October (2003)*

ii. *Buttyan, L. and Hubaux, J.P.: Security and Cooperation in Wireless Networks. Cambridge Univ. Press (2007)*

iii. *Dotzer, F., Fischer, L. and Magiera, P.: VARS: A Vehicle Ad-Hoc Network Reputation System. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. WoWMoM 2005. 13-16 June 2005 pp. 454-456 (2005)*

iv. *Fonseca, E. and Festag, A.: A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS, Technical Report NLE-PR-2006-19, NEC Network Laboratories, March (2006)*

v. *Ho, Y.H., Ho, A.H., Hamza-Lup, G.L. and Hua, K.A.: Cooperation Enforcement in Vehicular Networks. International Conference on Com-munication Theory, Reliability, and Quality of Service, 2008. CTRQ'08. June 29-July 5 pp. 7-12 (2008)*

vi. *Lee, S., Pan, G., Park, J., Gerla, M. and Lu, S.: Secure Incentives for Commercial Ad Dissemination in Vehicular Networks, MobiHoc'07, Canada, Sep 9-14 (2007)*

vii. *Li, F. and Wu, J.: FRAME: An Innovative Incentive Scheme in Vehicular Networks. Proc. of IEEE International Conference on Communications (ICC) (2009)*

viii. *Hernandez-Goya, C., Caballero-Gil, P., Molina-Gil, J. and Caballero-Gil P.:Cooperation Enforcement Schemes in Vehicular Ad-Hoc Networks. Lecture Notes in Computer Science. EUROCAST. Vol: No. 5717, Spain Feb 15-20, (2009).*

ix. *Liu, P. and Zang, W.: Incentive-based modeling and inference of attacker intent, objectives, and strategies, Proc. of the 10th ACM Computer and Communications Security Conference (CCS'03), Washington, DC, October pp. 179-189 (2003)*

x. *Shastry, N. and Adve, R.S.: Stimulating cooperative diversity in wireless ad hoc networks through pricing", IEEE Int. Conf. on Communications, June (2006)*

xi. *Srinivasan, V., Nuggehalli, P. and Rao, R.R.: Cooperation in Ad Hoc Networks, Proc. of Infocom, San Francisco, CA (2003)*

xii. *Wang, Z. and Chigan, C.: Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs. IEEE International Conference on Communications, 2007. ICC'07. 24-28 June pp. 3959-3964 (2007)*

xiii. *Wang, Z. and Chigan, C.: Cooperation Enhancement for Message Transmission in VANETs. Wireless Personal Communications: An In-ternational Journal Volume 43, Issue 1 October pp. 141-156 (2007)*

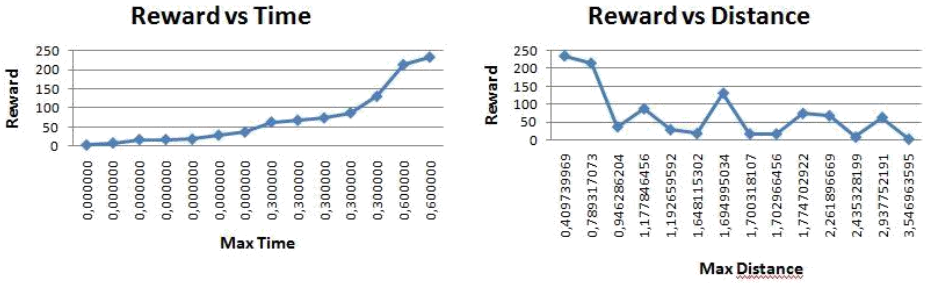

Fig. 2. Performance of the proposed scheme.

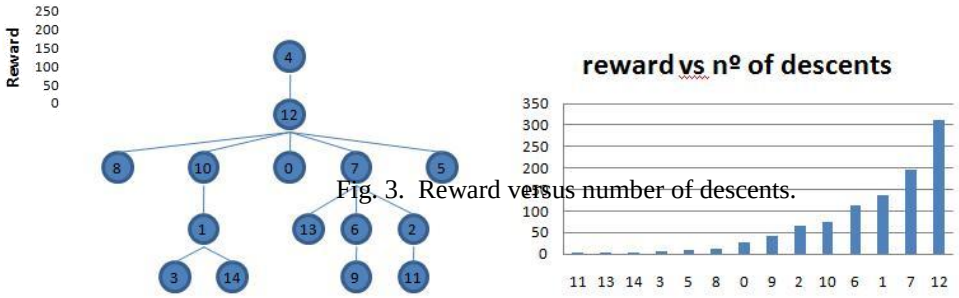

Fig. 3. Reward versus number of descents.