A SURVEY ON REPUTATION-BASED COOPERATION ENFORCEMENT SCHEMES IN WIRELESS AD HOC NETWORKS

Malamati Louta
Department of Informatics and Telematics, Harokopio University, 89 Harokopou str., Athens, Greece

Stylianos Kraounakis
Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani, Greece

Angelos Michalas
Department of Informatics and Computer Technology, Technological Educational Institute of Western Macedonia Kozani, Greece

Keywords: Wireless mobile ad hoc networks, Cooperation enforcement, Trust, Misbehaviour, Reputation mechanism.

Abstract: Mobile ad hoc networks rely on node cooperation to perform and support basic functions like packet forwarding, routing and network management. In general, nodes' misbehaviour can significantly degrade the performance of the network. Cooperation enforcement schemes are seen as a lightweight alternative to conventional security techniques, providing a "softer" security layer to protect basic networking operations. The aim of this paper is to survey representative cooperation enforcement schemes exploiting a reputation system proposed in related research literature. Their distinct features are analyzed and their relative merits and weaknesses are discussed.

1 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.

Mobile ad hoc networks rely on node cooperation to perform and support basic functions like packet forwarding, routing and network management, which 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.

In MANETs, cooperation enforcement schemes are seen as a viable, lightweight alternative to conventional security techniques involving cryptographically signed certificates exchange, providing a "softer" security layer to protect basic

Louta M., Kraounakis S. and Michalas A. (2010).
A SURVEY ON REPUTATION-BASED COOPERATION ENFORCEMENT SCHEMES IN WIRELESS AD HOC NETWORKS.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 90-93
DOI: 10.5220/0002986400900093

networking operations. Cooperation enforcement schemes 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, while the second provides for economic incentives. The aim of this paper is to survey representative cooperation enforcement schemes exploiting a reputation system proposed in related research literature. Their distinct features will be analyzed and the authors will discuss on their relative merits and weaknesses.

The rest of the paper is structured as follows. Section 2 presents six representative approaches proposed in the related research literature. Section 3 discusses on our findings, while section 4 concludes the paper and highlights our future plans.

2 REPUTATION SCHEMES

2.1 Watchdog - Pathrater

In (Marti, 2000) two extensions to the Dynamic Source Routing (DSR) protocol are introduced, namely the watchdog and the pathrater, so as to mitigate the effects of routing misbehaviour. The watchdog identifies misbehaving nodes by listening to the next node's transmission, exploiting promiscuous mode of operation. Each node maintains a buffer of recently sent packets; in case the packet is not forwarded on within a certain timeout or the overheard packet is different than the one stored in the buffer, the watchdog increments a failure counter for the node responsible for forwarding the packet. If the counter exceeds a certain threshold, the node is considered as misbehaving and the source is notified. The pathrater combines knowledge of misbehaving nodes with link reliability data to select the route most – likely to be reliable. Specifically, each node maintains a rating for every other node it knows about in the network and calculates a path metric by averaging the node ratings in the path, enabling thus the selection of the shortest path in case reliability information is unavailable. Negative path values indicate the existence of one or more misbehaving nodes in the path. If a node is marked as misbehaving due to temporary malfunction or incorrect accusation, a second-chance mechanism is considered, by slowly increasing the ratings of nodes that have negative values or by setting them to a non-negative value after a long-timeout.

2.2 CONFIDANT

In (Buchegger, 2002), the authors propose CONFIDANT, a routing protocol for MANET based on Dynamic Source Routing (DSR) protocol. Upon detection of the node's malice, its packets are not forwarded by normally behaving nodes, while it is avoided in case of a routing decision and deleted from a path cache. CONFIDANT architecture comprises 4 components residing on each node: the Monitor, the Reputation System, the Path Manager and the Trust Manager components. The Monitor component enables nodes to detect deviations of the next node on the source route by either listening to the transmission of the next node ("passive acknowledgement") or by observing route protocol behaviour.

In order to convey warning information in case of identification of a bad behaviour, an ALARM message is sent to the Trust Manager component, where the source of the message is evaluated. The rating is updated only if there is sufficient evidence of malicious behaviour that is significant for a node and that has occurred a number of times, exceeding a threshold to rule out coincidences (e.g., collisions). Evidence could come either from a node's own experiences through the Monitor system or from the Trust Manager in the form of Alarm messages. Second-hand information is attributed with low significance (by means of a constant weighting factor w) with respect to the first-hand information, irrespective of its source node.

Local rating lists and/or black lists are maintained at each node and potentially exchanged with friends. Black lists may be used in a route request, so as to avoid bad nodes along the way to the destination or to not handle a request originating from a malicious node and in forward packet requests, so as to avoid forwarding packets for nodes that have bad rating.

2.3 CORE

In (Michialdi, 2002), considering node's misbehaviour, the authors discern between selfish nodes that use the network, while not cooperating, saving, thus, battery for their own communications and malicious nodes that aim at damaging other nodes by causing network outage, while saving battery life is not a priority. They propose CORE, a collaborative reputation mechanism so as to enforce node cooperation in MANETs. CORE defines three different types of reputation: (i) Subjective Reputation, (ii) Indirect Reputation and (iii)

Functional Reputation. The former is the reputation observed locally by a node with regards to other nodes. The Indirect Reputation is reputation provided by nodes to other nodes. Subjective Reputation and Indirect Reputation are merged by means of a weighted combining formula in order to compute a final value of reputation concerning a specific evaluation criterion (e.g. packet forwarding) forming Functional Reputation, the last type of reputation considered. By combining different functional reputation values concerning different evaluation criteria, a global reputation value may be estimated. The subjective reputation is computed by giving more relevance to past observations than to recent ones. Subjective Reputation values are updated on the basis of a Watchdog mechanism, if misbehaviour is identified. Indirect Reputation values are updated by means of a reply message that contains a list of all entries that correctly behaved in the context of each function. In this study distribution of positive ratings is allowed so as to avoid potential denial of service attacks. In case reputation of an entity is negative, the execution of any requested operation will be denied by all other entities in the system. CORE does not provide for a second-chance mechanism.

2.4 SORI

SORI (Secure and Objective Reputation-based Incentive) scheme is proposed in (He, 2004) so as to encourage packet forwarding. SORI consists of three components, namely, neighbour monitoring (used to collect information about packet forwarding behaviour of neighbours), reputation propagation (employed so as to share information of other nodes with neighbours) and punishment (involved in the decision process of dropping packet action, taking into account the overall evaluation record of a node and a threshold so as to consider collision events). Reputation rating formation considers first-hand information weighted by a confidence value used to describe how confident a node is for its judgement on the reputation of another node and second-hand information weighted by the credibility of nodes which contribute to the calculation of reputation. Credibility of a node is defined on the basis of a node's behaviour as forwarder and not as a witness. Reputation rating itself is based on packet forwarding ratio of a node. SORI does not discriminate between selfish and misbehaving node terms. Both terms are used interchangeably throughout the paper. Additionally, SORI does not comprise a second-chance / redemption mechanism. Finally, SORI, in order to tackle with impersonation threats, constructs an authentication mechanism based on a one-way-hash chain.

2.5 OCEAN

OCEAN (Observation-based Cooperation Enforcement in Ad Hoc Networks) approach to selfishness in ad-hoc networks is to disallow any second-hand information exchanges (Bansal, 2003). Instead, a node makes routing decisions based solely on direct observations of its neighbouring nodes' interactions with it. OCEAN is designed on top of DSR protocol, may reside on each node in the network and hosts five components: Neighbour Watch (in order to observe the behaviour of the neighbours of a node), Route Ranker (estimating and maintaining ratings for each of the neighbouring nodes), Rank-based Routing (so as to avoid routes containing nodes in the faulty list), Malicious Traffic Rejection (rejecting all traffic from nodes it considers misleading so that a node is not able to relay its own traffic under the guise of forwarding it on somebody else's behalf) and Second Chance Mechanism (using a time-out based approach for removing a node from a faulty list after a fixed period of observed inactivity and assigning to it a neutral value). Once the rating of a node falls below a certain threshold, the node is added to the faulty list comprising all misbehaving nodes. In order to tackle selfish behaviour, the authors introduce a simple packet forwarding economy scheme, relying again only on direct observations of interactions with neighbours. Due to the usage of only first-hand information, OCEAN is more resilient to rumour spreading. Finally, the authors rely on recent work on proof-of-effort mechanisms and mandate that a new identity will be accepted only if the owner shows reasonable effort in generating that identity.

2.6 LARS

In (Hu, 2006), the authors propose LARS (Locally Aware Reputation System) to mitigate misbehaviour and enforce cooperation. Each node only keeps the reputation values of all its one-hop neighbours. The reputation values are updated on the basis of direct observations of the node's neighbours. If the reputation value of a node drops below an untrustworthy threshold, then it is considered misbehaving by the specific evaluator node. In such a case, the evaluator node will notify its neighbours about misbehaviour, by initiating a WARNING message. An uncooperative node is identified in the

neighbourhood region, in case a WARNING message issued by a node is co-signed by *m* different one hop-neighbours, where *m-1* is an upper bound on the number of nodes considered in the one-hop neighbourhood, in order to prevent false accusations and problems caused with inconsistent reputation values. Additionally, a fade factor has been introduced to give less weight to evidence received in the past. The misbehaving node is not excluded from the network for ever. After a time-out period, it is accepted, but with the reputation value unchanged so it would have to built its reputation by good cooperation.

3 DISCUSSION

After surveying the schemes proposed in related research literature, it is found that the different approaches lack unity. Each scheme is based on quite different assumptions, while the trust/reputation framework considered varies significantly in many aspects. Without being exhaustive, we could refer to information gathering for reputation computation exploiting only first hand information or both first-hand and second-hand information, propagation of second-hand information considering only positive, negative or both types of recommendation, degree of propagation, adopted model for reputation value computation, dishonest second-hand information provisioning, identification of misbehaving nodes, actions taken, node re-integration in the system, etc.). The presented schemes address in a quite different manner some of the aforementioned issues, while, to the best of our knowledge, a comprehensive list identifying all critical aspects and their implications to the design of a reputation-based cooperation enforcement scheme in MANETs is missing from related research literature. Additionally, even though simulation results are provided in most of the works surveyed, we could not reach to safe conclusions, as the simulation configurations, the parameters examined and measured and the assumptions that are made significantly vary. The authors believe that it would be quite interesting to analyze the performance of the examined cooperation enforcement with respect to network throughput realized, communication overhead introduced, time required for obtaining accurate reputation ratings/detecting misbehaving nodes, robustness against spurious ratings under a common reference scenario, which however entails a significant degree of difficulty.

4 CONCLUSIONS

In this paper, a representative set of reputation-based cooperation enforcement methods proposed in related research literature are surveyed, while their distinct features and relative merits and weaknesses are discussed. The authors conclude that the proposed schemes lack unity, while a comprehensive list of critical aspects and their implications to the design of a reputation-based cooperation enforcement scheme in MANETs is missing from related research literature. We plan to continue our work towards that direction, which could hopefully form the basis for defining a unified framework in the future.

REFERENCES

Bansal, S., Baker, M., 2003. “Observation-based Cooperation Enforcement in Ad hoc Networks”, arxiv:cs/0307012v2.

Buchegger, S. Le Boudec J.-Y.,, 2002. “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.*

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

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

Marti, S., Giuli, T. J., Lai, K., Baker, M., 2000. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, in *ACM MobiCom 2000 Conference.*

Michiardi, P., Molva, R., 2002. “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks”, in *CMS’02, Communications and Multimedia Security Conference.*