ISSN:0975-9646

A Review of Different Reputation Schemes to Thwart the Misbehaving Nodes in Mobile Ad Hoc Network

Suhas Sutariya[1], Prof. Prashant Modi[2]

[1]*M.Tech student, Department of Computer Engineering,*
U.V.Patel College of Engineering, Ganpat University, Kherva, Mehsana,India
[2]*Assistant Professor, Department of Informatin Technology,*
U.V.Patel College of Engineering, Ganpat University, Kherva, Mehsana,India

Abstract-In a mobile ad hoc network(MANET), a source node must rely on intermediate nodes to forward its packets along multi-hop routes to the destination node. Due to the lack of infrastructure in such networks, secure and reliable packet delivery is challenging. The presence of misbehaving nodes(sybils) results in degradation of network performance and makes it difficult in finding the routes between the nodes. By applying cooperation based schemes among nodes are seen as an effective schemes than conventional security schemes, which provide softer security layer to protect basic networking operations. The aim of this paper is to review the cooperation based schemes which exploits the reputation systems proposed in related research literature. The distinct features of the systems are analysed and merits and demerits are discussed.

Keywords:Reputation system, misbehaving node, manet

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.

The routing protocol plays a vital role in establishing route between the mobile nodes and maintenance of the routes in these networks. All nodes in an ad hoc network have to work mutually for executing the basic networking functions such as route discovery, route maintenance and multi-hop forwarding of packets. So the network performance becomes highly dependent on collaboration of all the participating nodes. More the number of nodes that participate in packet routing, greater is the aggregate bandwidth, shorter is the routing paths and minimum is the network partition. The mobile ad hoc network has a wide range of applications in diverse fields ranging from low power military wireless sensor networks to large scale civilian applications, emergency search and rescue operations.

The attacks launched against ad hoc networks are classified into passive and active attacks. In passive attacks, an attacker eavesdrop the network traffic in order to extract vital information from the data and control packets. Whereas in the case of active attacks, a malicious node disturbs the normal network operation by launching fabrication, modification or impersonation attacks.

In MANETs, cooperation based schemes are seen as a viable and lightweight alternatives to conventional security schemes involving cryptographically signed certificates exchange, providing a "softer" security layer to protect basic networking operations. Cooperation based 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 review representative cooperation based schemes exploiting a reputation system proposed in related research literature. Their distinct features will be analysed and the authors will discuss on their relative merits and demerits.

II. REPUTATION BASED SCHEMES IN MANETS

A. Watchdog and Path-Rater

Marti et al. [1] has two extensions to Dynamic Source Routing (DSR) protocol are introduced, namely the watchdog and the path-rater, 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 is maintaining buffer of the recently sent packets. In case, if packet is not forwarded within a certain timeout or 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 from certain threshold value, the node is considered as misbehaving node and the source node is notified. The path-rater combines the knowledge of misbehaving nodes with link reliability data to select the route most likely to be reliable. Negative path values are indicating the existence of one or more misbehaving nodes in the path. If current node is marked as misbehaving node due to temporary

malfunctioning 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.

Using the ns network simulator, these two techniques it increases through-put by 17% in the presence of up to 40% misbehaving nodes during moderate mobility, while increasing the ratio of overhead transmissions to data transmissions from the standard routing protocol's 9% to17%. During nodes' extreme mobility, watchdog and pathrater increased the network through-put by 27%, while increasing the percentage of overhead transmissions from 12% to 24%.

These results show that we can gain the benefits of an increased number of routing nodes while minimizing the effects of misbehaving nodes. In addition we show that this can be done without *a prior/trust* or excessive overhead.
This approach does not punish misbehaving nodes that do not cooperate and also relieves them of the burden of forwarding packets for other nodes.

B. CONFIDANT

Buchegger, 2002 et al. [2], 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.

Observable attacks on forwarding and routing in mobile ad-hoc networks can be thwarted by the suggested CONFIDANT scheme of detection, alerting, and reaction. Performance analysis by means of simulation shows a significant improvement in terms of good put when DSR is fortified with the CONFIDANT protocol extensions. The overhead for this increase is very low. The CONFIDANT protocol is scalable in terms of the total number of nodes in a network and performs well even with a fraction of malicious nodes as high as 60%.

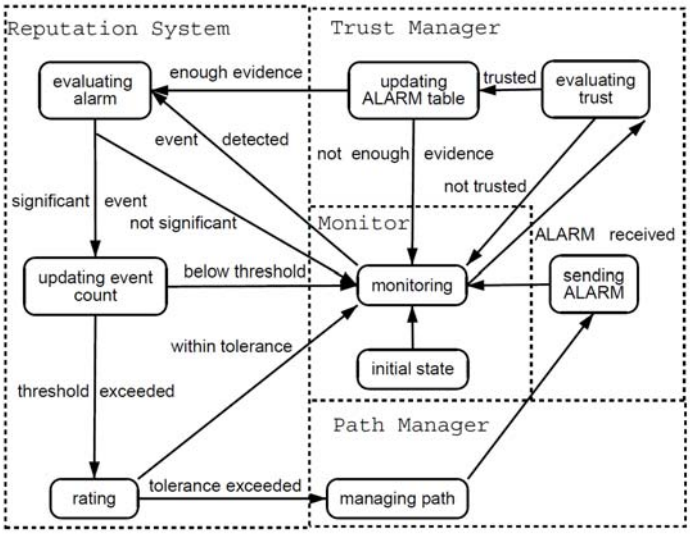

Figure. Trust architecture and finite state machinewithin each node.

C. CORE

Michialdi, 2002 et al. [3], 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.

The CORE scheme involves two types of protocol entities, a *requestor* and one or more *providers*, that are within the wireless transmission range of the *requestor*. The nature of the protocol and the mechanisms on which it relies assure that if a provider refuses to cooperate (i.e. the request is not satisfied), then the CORE scheme will react by decreasing the reputation of the provider, leading to its exclusion if the non-cooperative behaviour persists.

D. SORI

SORI[4] (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.

E. OCEAN

OCEAN[5] (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.

F. LARS

Hu,2006 et. al present in LARS[6] (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. The success of the scheme is on critical value of m.

G. PLRSA

Li et al. [7] proposed a Promiscuous Listening Routing Security Algorithm (PLRSA) to mitigate misbehaving nodes. PLRSA enables the promiscuous mode of every mobile host to intercept all the packets passing through the mobile host regardless of the destination address of the packet. Once when a node performs malicious behaviors, such as maliciously dropping of data packets or fabricating the spurious packets, the other nearby nodes may detect the spiteful behaviors. If the value of trust level is lower than a threshold defined by PLRSA then the node is considered as a malicious and further the malicious nodes are not considered for routing.

H. E-Herms

Zouridaki et al.[8] proposed a scheme called E-Hermes, in which each node determines the trustworthiness of the

other nodes with respect to reliable packet forwarding by combining first-hand trust information obtained independently of other nodes and second-hand trust information obtained via recommendations from other nodes. First-hand trust information for neighbor nodes is obtained via direct observations at the MAC layer whereas first-hand information for non-neighbor nodes is obtained via feedback from acknowledgment's sent in response to data packets.

The trustworthiness of the recommendations and recommenders is evaluated. The concept of trustworthiness is then extended to the notion of an opinion that a given node has about the forwarding behavior of any arbitrary node by combining first-hand and second-hand trust information. A potential problem arises when a node behaves well with respect to some flows, but behaves badly with respect to other flows. The E-Hermes scheme may not be able to compute accurate trustworthiness values in this case.

I. LMRSA

Gopalakrishnan et al. [9] proposed a Local Monitoring based Reputation System with Alert (LMRSA) to mitigate the misbehaving nodes in MANETs. This scheme derives the trustworthiness based on the direct observation experienced by a node from its next hop neighbors and also it does not exchange the trust values with the rest of the nodes in the network. This scheme generates an explicit alert and sends it to source node of the monitored transmission, whenever it declares its next hop node as a misbehaving node. This enables the packet originating node to select an alternate route for its current transmission, which in turn increases the overall network throughput but it also suffers from the same disadvantages as mentioned in watchdog/path rater scheme.

J. CARS

Collaborative Alert in a Reputation System (CARS)[10] which is based on neighborhood monitoring approach to detect and isolate the colluding packet droppers. This scheme hows promising result due to its unique approach in monitoring the neighboring nodes along with explicit alert mechanism.

K. NMCAM

Gopalakrishnan et al [11] proposed the mechanism named Neighborhood Monitoring Based collaborative Alert Mechanism(NMCAM) shows the effectiveness of system in finding shorter and better routes without containing misbehaving nodes in it. The false detection and malicious drop which occurred in the network due to the presence of misbehaving nodes has been reduced greatly. It shows the efficiency of packet monitoring and evaluation procedure along with the explicit route error generation. This scheme is immune to colluding node misbehaviour due to timely generation of an explicit route error packet by the neighbouring nodes to inform the source node of the packet about the misbehaving link along with the dissemination of misbehaving node information. Based on the other literature survey, this is the work which thoroughly analyses the impact of different kind of misbehaving nodes under group mobility scenario. This scheme is best suited for an un-managed self organized ad hoc network but it can also be used in a managed ad hoc network that lacks the centralized control based trusted security mechanism or requires monitoring the correct functioning of neighbouring nodes.

III. 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 analyse 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.

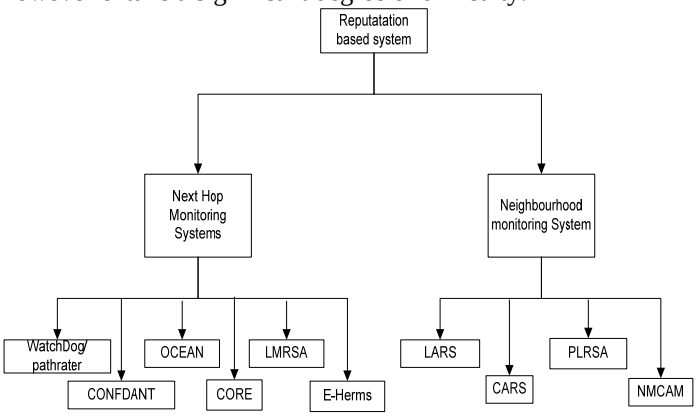

Fig. Various schemes Reputation based system

The schemes [A-D,H,I] are based on next hop monitoring, in which the nodes except the destination and

its previous hop in the source route of the packet has to monitor the behaviour of its next hop in order to identify the node misbehaviour, but the monitoring method employed by these schemes have the same disadvantages as mentioned in [A]. Whereas the schemes [F,G,J] employs neighbourhood monitoring approach, which adds flexibility in monitoring by allowing a node to monitor the neighbouring transmissions even if those transmissions does not involves it.

IV. CONCLUSION

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 some of the critical aspects and their implications to the design of a reputation-based cooperation enforcement scheme in MANETs may be 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

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

[2] 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*.

[3] 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*.

[4] 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*.

[5] Bansal, S., Baker, M., 2003. "Observation-based Cooperation Enforcement in Ad hoc Networks", arxiv:cs/0307012v2.

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

[7] Li, J-S., Lee, C-T., 2006. "Improve Routing Trust with Promiscuous Listening Routing Security Algorithm in Mobile Ad Hoc Networks", *Journal of ELSEVIER Computer Communications*, pp. 1121-1132.

[8] Zouridaki, C., Mark, B., Hejmo, M., Thomas, R., 2009. "E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks", *Journal of ELSEVIER Ad Hoc Networks* pp. 1156–1168.

[9] Gopalakrishnan, K., Rhymend Uthariaraj, V., 2010. "Local Monitoring based Reputation System with Alert to Mitigate the Misbehaving Nodes in Mobile Ad Hoc Networks", *In: Das, V.V., Vijaykumar, R. (Eds.) ICT 2010.Part II, CCIS*, vol. 101, pp. 344–349. Springer, Heidelberg.

[10] Gopalakrishnan, K., Rhymend Uthariaraj, V., 2011. "Collaborative Alert in a Reputation System to Alleviate Colluding Packet Droppers in Mobile Ad Hoc Networks", *In: Meghanathan, N., Kaushik, B.K., Nagamalai, D. (Eds.) CCSIT 2011. Part I, CCIS*, vol. 131, pp. 135–146. Springer, Heidelberg.

[11] K. Gopalakrishnan & Rhymend Uthariaraj, in V.. 2011, "Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad-Hoc Network ", European Journal of Scientific Research ISSN 1450-216X Vol.57 No.3 pp.411-425.