ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Survey on Secure Cooperation Mechanisms on Multihop Cellular Networks

Manasa N [*1], Pavan Kumar P[2]

[*1] PG Student, Department of CSE, CMR Institute of Technology, Hyderabad, India

[2] Associate Professor, Department of CSE, CMR Institute of Technology, Hyderabad, india

manasachowdary@gmail.com

Abstract

Multihop Cellular Networks (MCN) combines the power of single hop networks and ad hoc networks. Data transmission in MCN is through the different hops of the networks. Due to this factor MCN hinge on the cooperation of nodes for routing and forwarding because all the packets are forwarded multihop fashion. . The node may become selfish node yielding non cooperation in the network. In order to encourage co operation between nodes many incentive schemes are proposed. This paper provides a survey about various schemes proposed for cooperation in multihop cellular networks.

Keywords: Cooperation, Multi hop cellular networks, Selfishness

Introduction

A multihop cellular network (MCN) is a self organized network formed by a collection of mobile nodes without fixed infrastructure management. MCN is good alternative to the conventional Single-hop Cellular Network (SCN) by combining the features of SCN and ad-hoc networks. In this connection between source and destination is established over a multi-hop path. The packets in the MANET are forwarded in a multi-hop fashion, requiring the contribution of every participant nodes. Recent research shows that the short distance transmission feature of MANET can improve the traditional cellular network in terms of throughput, delay and power efficiency. However, since the mobile nodes in this network are constrained with limited resources, such as CPU, battery, channel bandwidth and etc, some nodes in the network might not be willing to cooperate for the packet transmission, in order to save their resources. Since the MANET is predicable to be deployed for civilian application where no single authority exists for the packets transmission management, the cooperative behaviors between these nodes cannot be guaranteed. There might be some nodes intending not to forward packets to save resources for their own use but still seek to use other's resources. The presence of only a few such selfish nodes can dramatically degrade the performance of an entire system. Two types of uncooperative nodes might exist in the system: malicious nodes and selfish nodes. The term malicious refers to the group of nodes that intentionally try to attack the system or break the network. On the other hand, the term selfish refers to the nodes that try to gain help from the network without willing to pay back the help received. Both malicious and selfish nodes are considered as misbehaving nodes. A fairness issue arises when selfish nodes take advantage of the cooperative nodes without any contribution to them. The selfish behavior also significantly degrades the network performance, which may result in failure of the multihop communications.

Two kinds of systems: reputation-based schemes and pricing-based schemes have been proposed to deal with the in cooperative behaviors. Reputation-based schemes set up a reputation threshold to distinguish the selfish nodes from cooperative nodes. Nodes whose reputation values are higher than a threshold are regarded as cooperative nodes, while nodes whose reputation values are lower than the threshold are selfish nodes. Nodes provide services to high-reputed nodes, and refuse to provide services to low-reputed nodes. Therefore, as long as a node has a reputation value that just a little higher than the threshold, it can always be served. This is not fair to high-reputed nodes with different level since they receive the service with the same quality. Reputation-based schemes need to have a complement method to help them wisely punish selfish nodes, and reward altruistic nodes. This paper provides a overview of various techniques used for enhancing the cooperation between the nodes.

Cooperation Enhancement Mechanisms

To enforce cooperation and discourage misbehaviour of nodes, three major models have been

ISSN: 2277-9655
Impact Factor: 1.852

developed: a) Reputation based, b) Trust based and c) Credit based models, as shown in Figure 1. By utilizing the past behaviour of end-users, reputation and trust based schemes enable a node to decide whether other nodes are trustworthy and cooperative. Eventually nodes having high reputation or trust are given services and nodes having low reputation or trust are isolated from the network. In credit based schemes nodes usually pay for services; payments are made in the form of virtual currency. Nodes are buyers and/or sellers of the packet forwarding services. Nodes require credit to forward their packets. Credit based schemes have some issues that make them impractical for use in MCNs. Firstly; they are not scalable due to the central virtual bank. Secondly, these models need some form of tamper proof hardware on each node. Reputation or trust based models on the other hand do not need any centralized entity, such as a virtual bank, or any tamper proof hardware. As a consequence they can be implemented in a distributed manner to increase scalability, making them much more suitable for use in MCNs.

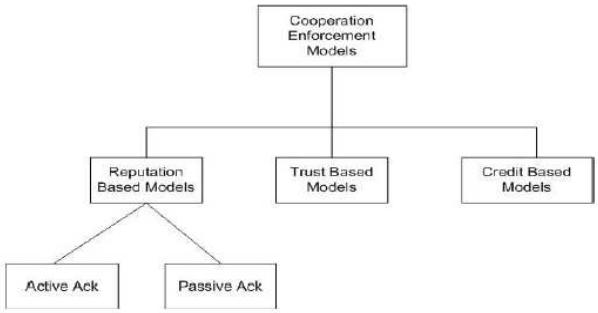

Figure 1 Cooperation enforcement Mechanisms in MCN

A reputation based system collects first-hand or direct information by monitoring its immediate neighbors for direct interactions. To strengthen a node's decision regarding another node's behavior, whether selfish or benign, second-hand information is collected from the deciding node's neighbors. However more weight is given to the direct interaction information, to mitigate the possibility of a neighbor node being deceitful. The core part of the reputation based models is monitoring or observation of one hop neighbors. Due to the fact that a node can trust nobody but itself, it gives more weight to direct observations, which are called first hand information. The more perfect and reliable the monitoring component is the more accurate and efficient the detection of a misbehaving node will be. However, due to the complex and unpredictable nature of a mobile ad hoc network, it is very difficult to have a perfect monitoring system at low cost (where cost may be measured as energy or some other metric). In this document we have tried to ramify reputation schemes based on the monitoring components that can be referred to as active and passive acknowledgments. Both have their own advantages and disadvantages.

Reputation Based Method

Reputation mechanisms are based on the behavior of a node in the network. Each node has a reputation value that reflects its behavior. This value is stored and calculated by other nodes that watch its behavior. Some of the key points that need to be addressed under this class are:

Trust vs. Reputation: Reputation rating represents how well a node behaves, and is used to decide whether the node is cooperative or misbehaving. On the other hand, trust rating represents how honest a node is, used to decide whether the node is trustworthy or not, thus the indirect reputation message from the node is accepted or not

Direct vs. Indirect Trust (Reputation): Direct Reputation (First Hand Information) is obtained by direct observation. A node monitors the behavior of other nodes usually in one-hop to see if it works well. On the other hand, Indirect Reputation (Second Hand Information) obtains reputation information about a node from other nodes in the network. The acceptance or rejection of this information is based on the trust level of the sender node.

Global vs. Local Reputation: Global reputation refers to the case where every node knows the reputation of every other node in the network. This is achieved by exchanging indirect reputation messages among the network. In local reputation, however, information is based only on direct observations of one-hop neighbors. Any secondhand reputation exchanges are disallowed.paragraphs must be indented.

Reputation values are stored for each node and may be shared as second hand information with other neighbours as well. Eventually nodes having high reputation get services whereas nodes having low reputation are isolated from the network.

CONFIDENT

Buchegger and Le Boudec proposed a scheme, called CONFIDANT [1], designed as an extension to an ondemand routing protocol, such as the DSR. CONFIDANT facilitates monitoring and reporting for a route establishment that avoids the misbehaving nodes. It is based on the assumption that the packets of misbehaving nodes are not forwarded by fair nodes. If, however, a node was incorrectly accused or turns out to be a repentant and no longer malicious, re-integration

ISSN: 2277-9655
Impact Factor: 1.852

into the network is possible. CONFIDANT employs four functional components relying on each node, which include: (a) a monitor, (b) reputation records for first-hand and trusted second-hand observations about routing and forwarding function of other nodes, (c) trust records to control the trust that is given to received warnings, and, (d) a path manager to take routing decisions that avoid malicious nodes. Nodes monitor their neighbors and change reputations accordingly. Specifically, a node can detect selfish behavior of the next node in the source route either directly, by promiscuously sensing the transmission of the next node, or indirect, by observing routing protocol misbehavior. The Monitor component registers these deviations. As soon as a specific misbehavior occurs, the Reputation System is called, and ALARM messages are sent by the Trust Manager. Outgoing ALARMS are generated by the node itself after having experienced, observed, or received a report of malicious behavior of another node. They convey warnings of malicious nodes presence. The recipients of the ALARM messages, so-called friends, are maintained in a friends list. Incoming ALARMs that originated from 'strangers,' are checked for trustworthiness before triggering a reaction. The disadvantage here is the requirement of a pre-existed trust relationship. If there is sufficient evidence that the node reported in the ALARM is malicious, the information is sent to the Reputation System. This manages a table consisting of entries corresponding to nodes and their ratings. A rating is modified if two conditions coincide: (i) there is sufficient evidence of malicious behavior, and, (ii) a misbehavior occurs a number of times, exceeding a threshold to rule out coincidences. The ranking of a node is changed according to a rate function. CONFIDANT does not use tamper-proof hardware. For a misbehaving node, it is hard to know the entries of its reputation in other nodes or to modify its reputations. However, it is still possible to alter the values of α and β or to change its identity. Only identities generated with cryptographic means can reduce this threat. The Bayesian approach reduces the impact of tampering with α and β. If values are not compatible with each other the algorithm will just ignore them. Evil nodes could only change the values with a small amount which is tolerable by the system.

CORE

This scheme, introduced by Michiardi and Molva [3], relies on the DSR routing protocol. It stimulates node collaboration through monitoring of the cooperativeness of nodes and a reputation mechanism. It uses first and second-hand experiences, combined by a specialized function. This function is used by the Watchdog mechanism for the evaluation of other nodes' behavior. If the observed behavior is different than the outcome of this function then the rating of the observed node is altered. Each node of the network monitors the behavior of its neighbors, with respect to the requested function, and collects observations about the execution of that function. These observations are recorded to the Reputation Table (RT), maintained by each node. Thus, each node maintains one RT for each monitored function. Finally, a global RT is used to combine the different RVs calculated for the different functions. CORE differentiates the RVs between subjective reputation ([_1, 1]), indirect reputation (positive reports by others), and functional reputation (e.g., when packet forwarding has greater effect than routing), which are weighted to provide a combined RV.

The formula used to evaluate the RV avoids false detections by using an aging factor that gives more relevance to past observations. However, such an approach is vulnerable to an attack where a node can build up a good reputation before misbehaving. The RVs evaluated for each entry of the RT vary. A positive RV is decremented along time. So, if a node enters in an idle mode, its reputation has to be decreased, even if during the active time (i.e., when communicates) it cooperates to the network operation. Reputation is decreased until it reaches a null value, which corresponds to a neutral behavior

The CORE scheme is immune to attacks performed using the mechanism itself: no negative ratings are spread, and, thus, it is impossible for a node to maliciously decrease another node's reputation Misbehaving nodes can, however, be reintegrated in the network if they increase on purpose their reputation, by cooperating to the network operation. CORE does not discriminate malfunction and misbehaving nodes

SORI

The secure and objective reputation-based incentive scheme for ad-hoc networks, introduced in [7], focuses on the packet forwarding function. SORI, consists of three basic components: Neighbor Monitoring, Reputation Propagation and Punishment. A promiscuous mode is assumed, and a node is capable of overhearing the transmissions of its neighbors and to maintain a neighbor node list. SORI combines features of the fist-hand schemes and those that use reputation spreading. In SORI the nodes exchange reputation information only with their neighbors. This way a no-cooperative node will be punished by all of its neighbors (who share the reputation information about its misbehavior), instead of just the ones who are directly affected by this node.

OCEAN

The observation-based cooperation enforcement in ad hoc networks, proposed in [7], introduces an

ISSN: 2277-9655
Impact Factor: 1.852

intermediate layer that resides between the network and the MAC layers. This layer helps the nodes to make intelligent routing and forwarding decisions. It is designed on the DSR level, but its principles can be applied to other routing protocols, as well. OCEAN relies only on first-hand observations. Every node maintains ratings for each neighboring node and monitors their behaviors through promiscuous observations. Due to empirical studies, the absolute value of a decrement is chosen to be bigger than the value of an increment. When the rating of a node drops below a threshold, called faulty threshold the node is added to a faulty list. This list is constructed using the node's personal experiences and is attached (as a field called avoid-list) to the route request (RREQ) message of the DSR protocol in order to be flooded. A route is rated good or bad, based on whether the next hop in the route belongs to the avoid-list. The receiver of an RREQ decides to drop it or to further process it (through relaying or a route reply), if the intersection of the avoid-list and the DSR route in the RREQ packet is void. In this way, each node along a route, makes its own decision about the trustworthiness of other nodes, and has control only over routes that it belongs to. Every node rejects the data packets arrived from the nodes belonging to its faulty list. Thus, misbehaving nodes are eventually isolated. However, a secondchance mechanism is used to allow nodes that misbehaved in the past to become operational again. After a certain period, a misbehaved node is excluded from the faulty list and assigned with a neutral rating. OCEAN uses a different policy to deal with nodes that do not participate in the route discovery process. This policy, affected by the credit-based models, requires no tamper-proof hardware or a central server. Each node measures the behavior of its neighbors by directly interacting with them. Nodes track the forwarding balance with their neighbors by maintaining one counter, called chip count, per node. The counter increases when requesting a node to forward a packet and decreases with an incoming request from that node. Assume that a node B did not participate on the establishment of route with a source node A. If B demands from A to forward its packets, then, A will punish B and reject its requests, as long as the chip count for B is low. This policy is considered unfair for nodes belonging to the perimeter of the MANET, since they are not frequently required to forward messages on behalf of others. Penalizing these nodes might cause the network to shrink. To overcome such phenomena, the OCEAN introduces a chip accumulation rate (CAR) parameter, which expresses the rate at which all chip count in the network are increased per unit time. Thus, the forwarding of the packets sent by circumferential nodes is enforced, even at a reduced rate. CAR can't be adjusted easily and there no mechanism to prevent a node to change it at will.

Credit Based Method

A. ***Sprite***

The simple, cheat-proof, credit-based system for mobile ah-hoc networks was proposed in Reference [4]. It does not require tamper-proof hardware to prevent the deviation of payment units, but incorporates a centralized credit clearance service (CCS). When receiving a packet, a node keeps the signed receipt of this packet, which was generated by the source node. Sprite assumes that each node has a public key certificate published by a CA. When the node has a fast connection to the CCS it reports the packets that it has received by uploading its collected and signed receipts. Sprite prevents any cheating by making it unattractive even in the case of collusion. When a node sends its own packets it loses a credit (virtual money), because other nodes incur a cost to forward these packets. In order to gain a credit and be able to send packets later, a node must forward packets on behalf of others. CCS charges the sender based on the number of receipts, the number of intermediate nodes left to reach the destination, if any, and whether the destination has sent a receipt. The mechanism is designed to be resilient against the following selfish actions: (1) after receiving a packet, the node saves a receipt but does not forward it, (2) the node has received a packet but does not report the receipt, and, (3) the node does not receive a packet but falsely claims that it has received it.

B. ***Token Based Cooperation Enforcement Schemes***

This scheme, introduced in Reference [6], protects both routing and packet forwarding in the context of the AODV protocol. It is self-organized, without assuming any a-priori trust between the nodes, or the existence of any centralized trust entity. It isolates the misbehaving nodes and employs threshold cryptography to enhance the tolerance against these nodes. The scheme is fully localized (one hop), and its creditbased strategy produces overhead that is significantly decreased when the network is not harmed. It assumes that the nodes operate promiscuously. Multiple attackers may coexist, but it is assumed that they collude locally. However, the collusion impact is minimized, since it is assumed that each node has a unique id, and the underlying cryptography is strong. The system's secret key is shared among the network nodes, and each node maintains only a limited portion of it. Each node carries a token, signed with the system's secret key as derived from the threshold cryptography process.

ISSN: 2277-9655
Impact Factor: 1.852

C. **Ad hoc VCG**

Energy-efficiency is a parameter of high importance for the MANET routing protocols . It ensures that a packet gets routed along the most energy-efficient path. The total energy of a routing path is the sum on the emission energy levels used at the source and at each intermediate node. The ad hoc-VCG scheme, proposed in Reference [5], is a credit-based model which deals with this issue and introduces a second-best sealed type of auction. The ad hoc-VCG works on top of the DSR. It consists of two distinct phases. During the route discovery phase, a weighted graph is computed. The vertices represent network nodes; the weighted directed edges correspond to the payments a relaying node has to receive to forward a packet along this edge. A destination node collects all the weights of the edges, and then computes the shortest path in the graph from the source to destination, which corresponds to the most energy-efficient path. During the data transmission phase, packets are forwarded along the shortest path and payments are made to the intermediates.

Conclusion

The main purpose of any cooperation enforcement scheme is to detect and isolate misbehaving nodes. In other words any node must face the consequences of its actions. Selfish or misbehaving nodes degrade overall system performance and pose a serious threat to multihop routing in MANETs. Reputation based models play an important role in detecting and isolating selfish nodes. In this paper we categorized reputation based schemes. Finally, we discussed their pros and cons as well as some other important identity related issues and suggested some directions for future work.

References

[1] Buchegger S, Le Boudec JY. Performance analysis of the CONFIDANT protocol. In Proceedings of 3rd ACM International Symposium, on Mobile Ad Hoc Networking and Computing, June 2002

[2] Dewan P, Dasgupta P, Bhattacharya A. On using reputations in ad hoc networks to counter malicious nodes. In Proceedings of QoS and Dynamic Systems, July 2004.

[3] Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of 6th IFIP Communication and Multimedia Security Conference, September 2002.

[4] Zhong S. Chen , Yang R Sprite : a simple cheat proof credit based system for mobile ad hoc networks, In Proceedings of INFOCOM 2003, April 2003.

[5] Anderegg L Eidenbenz S Ad hoc VCG: a truthful and cost efficient routing protocol for mobile ad hoc networks with selfish agents. In Proceedings of 9th Annual International conference on Mobile Computing and Networking September 2003.

[6] Yang H Meng X, Lu S Self Organized Network Layer Security in mobile ad hoc networks. In Proceedings of ACM WiSe02, September2002.

[7] Bansal S, Baker M . Observation Based Cooperation Enforcement in Ad hoc Networks. Technical Report, Stanford University, 2003.