Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.495 – 500

SURVEY ARTICLE

Survey on Quality Analysis of Cooperation Incentive Strategies in MANET

K Savitha Rohini[1], S Dhanasekar[2]

[1]P.G Scholar, Department of Computer Science and Engineering, Anna University, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University, India

[1] rohini.savitha@gmail.com; [2] dhnasekar.sethupathi@gmail.com

Abstract*— In mobile ad hoc networks (MANETs), tasks are conducted based on the cooperation of nodes in the networks. However, since the nodes are usually constrained by limited computation resources, selfish nodes may refuse to be cooperative. Reputation system is one of the main solutions to the node non-cooperation problem. A reputation system evaluates node behaviours by reputation values and uses a reputation threshold to distinguish trustworthy nodes and untrustworthy nodes. Although this system has been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the systems. We propose a protocol called Enhanced Reverse Ad Hoc On Demand Vector Routing Protocol (ERAODV), which uses Hybrid Reputation System (HRS). A Hybrid Reputation system is an enhanced version of Classical Reputation System (CRS). Unlike the CRS it takes into account all the reputation values from the node to determine whether it is trustworthy or not.

***Keywords*—MANET; Reputation System; Price Based System; Quality Analysis; Multipath Routing**

I. Introduction

A computer network is created to provide a means of transmitting data, sometimes essential data, from one computer to another. There are two types of networks, based on the connections made. They are wired and wireless networks.

A wired network is one in which all the components are connected with network cables. For mobility, Wireless LAN technology is a key enabling technology that allows computers to extend their existing network into areas where hardwiring would be expensive or difficult. It allows users to achieve total PC portability and location independence.

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made

© 2014, IJCSMC All Rights Reserved

dynamically on the basis of network connectivity. There are two types of routing protocols used in MANET, they are: Proactive and Reactive protocols.

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. Our aim is to design a new protocol based on Reverse Ad hoc On Demand Vector (RAODV) called as Enhanced Reverse Ad hoc On Demand Vector (ERAODV) which provides better security compared to AODV & RAODV.

II. LITERATURE REVIEW

Balakrishnan, Jing Deng, and Pramod K. Varshney, [3] 2005, Proposed as, Securing the Mobile Ad Hoc Networks (MANETs) in an untrustworthy environment is always a challenging problem. In recent years, MANETs have become a very popular research topic. MANETs are attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. However, performing network functions consumes energy and other resources. To save its energy a node may behave selfishly and uses the forwarding service of other nodes without correctly can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance process but refuse to forward packets. In this survey they use Specific behavior pattern creation that would let to evaluate neighbour behaviour. There are many methods deal with the selfish behavior of the nodes and this paper compares different methods available for reducing the effect of selfish nodes in MANET. Even though, it has some limitations. In our proposed system we are going to implement a hybrid reputation system which overcomes the limitations of Specific behaviour pattern and provides security by means of multi hop pattern.

Prashant Dewan, Partha Dasgupta, and Amiya Bhattacharya, [6] 2004, Proposed as, Nodes in Mobile Ad Hoc Networks (MANETs) have a limited transmission range. Hence the nodes except their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumptions that if a node promises to relay a packet, it will relay it and it will not cheat. This assumption becomes invalid when the nodes in the network have tangential or contradictory. The reputation of the nodes, based on their previous relaying history, cannot only be used to increase the throughput of an ad hoc network but also to motivate nodes to cooperate. The cost of this improvement is increased number of route requests. The throughput can be further improved at the cost of extra messages, by making the nodes exchange their reputation databases using cryptographic protocols for ascertaining the credibility of the source of information and the correctness of the reputation information obtained. Our proposed project uses the quantitative models for calculating threshold which will increase the usability of nodes.

M.T. Refaei, L.A. DaSilva, M. Eltoweissy, and T. Nadeem, [7] 2010, Proposed as, Reputation management systems have been proposed as a cooperation enforcement solution in ad hoc networks. Typically, the functions of reputation management (evaluation, detection, and reaction) are carried out homogeneously across time and space. However, the dynamic nature of ad hoc networks causes node behavior to vary both spatially and temporally due to changes in local and network-wide conditions. When reputation management functions do not adapt to such changes, their effectiveness, measured in terms of accuracy (correct identification of node behavior) and promptness (timely identification of node misbehavior), may be compromised. So they propose an adaptive reputation management system that realizes that changes in node behavior may be driven by changes in network conditions and that accommodates such changes by adapting its operating parameters. They introduce a time-slotted approach to allow the evaluation function to quickly and accurately capture changes in node behavior. Finally compare the proposed solution to a nonadaptive system, showing the ability of our system to achieve high accuracy and promptness in dynamic environments. The results obtained show that our adaptive system can operate under a wide range of network conditions and yields low false positives and false negatives with fast detection, thus, reducing the impact of misbehaving nodes on the network. All though it have some limitation, the effectiveness of the adaptive reputation management system under more complex network environments where network conditions, network structure (e.g., topology, node density, etc.), and nodes' intent (i.e., to act cooperatively versus to misbehave) may change rapidly are difficult.

Z. Li and H. Shen, [9] 2011. Proposed as, encouraging cooperative and deterring selfish behaviors are important for proper operations of MANETs. For this purpose, most previous efforts either rely on reputation systems or price systems. However, both systems are neither sufficiently effective in providing cooperation incentives nor efficient in resource consumption. Nodes in both systems can be uncooperative while still being considered trustworthy. Also, information exchange between mobile nodes in reputation systems and credit circulation in price systems consume significant resources. This paper presents a hierarchical Account-aided Reputation Management system (ARM) to efficiently and effectively provide cooperation incentives. ARM builds a hierarchical locality-aware DHT infrastructure for efficient and integrated operations of both reputation and price systems. The infrastructure helps to globally collect all reputation information in the system, which helps to calculate more accurate reputation and detect abnormal reputation information. Also, ARM co-ordinately integrates resource and price systems by enabling higher-reputed nodes to pay less for their received services. Theoretical analysis demonstrates the properties of ARM. Simulation results show that ARM outperforms both a reputation system and price system in terms of effectiveness and efficiency.

P. Michiardi and R. Molva, [8] 2002, Proposed as, Countermeasures for node misbehavior and selfishness are mandatory requirements in MANET. Selfishness that causes lack of node activity cannot be solved by classical security means that aim at verifying the correctness and integrity of an operation. We suggest a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET to prevent selfish behavior. Each network entity keeps track of other entities' collaboration using a technique called reputation. The reputation is calculated based on various types of information on each entity's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented. The generic mechanism can be smoothly extended to basic network functions with little impact on existing protocols. They focused on MANET where there is a lack of a priori trust relationship between mobile nodes. Counter measures against node misbehavior in general and denial of service attacks in particular is our very first concern. This paper suggested a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET and to prevent passive denial of service attacks due to node selfishness.

S. Bansal and M. Baker,[2] 2003, Proposed as, Ad hoc networks rely on the cooperation of the nodes participating in the network to forward packets for each other. A node may decide not to cooperate to save its resources while still using the network to relay its traffic. If too many nodes exhibit this behavior, network performance degrades and cooperating nodes may find themselves unfairly loaded. Most previous efforts to counter this behavior have relied on further cooperation between nodes to exchange reputation information about other nodes. If a node observes another node not participating correctly, it reports this observation to other nodes who then take action to avoid being affected and potentially punish the bad node by refusing to forward its traffic. Unfortunately, such second-hand reputation information is subject to false accusations and requires maintaining trust relationships with other nodes. The OCEAN techniques for detecting and mitigating misleading routing behavior in ad hoc networks. The goal was to study how far we can get using only direct observations of neighbors. We find that this scheme works surprisingly well, in terms of network throughput, considering its simplicity compared to schemes that share second-hand reputation information throughout the network. Compared to such reputation schemes, OCEAN is more sensitive to the tuning of some parameters, and it fails to punish misbehaving nodes as severely, but it performs almost as well, and sometimes even better, across a wide range of degrees of mobility. How we can provide more effective infrastructure-free authentication in ad hoc networks assuming that identities need not be entirely stable at the routing level, but that spoofing of other nodes is unacceptable.

S. Zhong, J. Chen, and Y.R. Yang,[5] 2003, Proposed as, Sprite, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in mobile ad hoc networks. This system provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, this system does not require any tamperproof hardware at any node. The system to provide incentive to mobile nodes to cooperate. Determines payments and charges from a game-theoretic perspective, and showed that the system motivates each node to report its behavior honestly, even when a collection of the selfish nodes collude. They also modelled the essential component of our system as the receipt-submission game, and proved the correctness of our system under this model. As far as, this is the first pure-software solution that has formal proofs of security. The result works for packet forwarding in unicast, and they extended it for route discovery and multicast as well. We also implemented a prototype of our system and showed the overhead of our system is insignificant. Simulations and analysis of the power-and-credit-conservative nodes showed that the nodes can cooperate and forward each other’s messages, unless the resource of the nodes is extremely low.

Luzi Anderegg, Stephan Eidenbenz, [4] 2003, Proposed as, This literature introduces a game-theoretic settings for routing in a Mobile Ad Hoc Network that consist of greedy, selfish agents who accept payments for forwarding data for other agents if the payment cover their individual costs incurred by forwarding data. And they propose Ad Hoc VCG, a reactive routing protocol that achieves the design objectives of truthfulness and cost efficiency in a game-theoretic sense by paying to the intermediate nodes a premium over their actual costs for forwarding data packets. This literature analyzes a very natural routing protocol that is an adaption of the Packet Purse Model with auctions in settings and show that, unfortunately, it does not achieve cost-efficiency or truthfulness. Though the Packet Purse Model can simulate nodes to be cooperative, most systems fail to provide a way to know the service quality of a node. Moreover they fail to punish a selfish and wealthy node that earns many credits by being cooperative but drops other packets later on.

In our proposed system we totally ignore the use of such price based Packet Purse Model and make use of the hybrid reputation system to identify the greedy and selfish nodes and also to know the service quality of nodes.

K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, [12] 2007, Proposed as, to investigated the performance degradation caused by such selfish (misbehaving) nodes in MANETs. The 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Compared with other approaches to combat the problem, such as the overhearing technique, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in MANETs. One advantage of the 2ACK scheme is its flexibility to control overhead with the use of the Rack parameter. the focused only on link misbehavior. It is more difficult to decide the behavior of a single node. This is mainly due to the fact that communication takes place between two nodes and is not the sole effort of a single node. Therefore, care must be taken before punishing any node associated with the misbehaving links. When a link misbehaves, either of the two nodes associated with the link may be misbehaving. In order to decide the behavior of a node and punish it, we may need to check the behavior of links around that node.

Wei Yu, and K.J. Ray Liu, [10] 2007 Proposed as, In Autonomous Mobile Ad Hoc Networks, nodes belong to different authorities and pursue different goals; therefore cooperation among them cannot be taken for granted. Meanwhile, some nodes may be malicious, whose objective is to damage the network. This literature proposes a joint analysis of cooperation stimulation and security in Autonomous Mobile Ad Hoc Networks under a Game-Theoretic framework, which allows integrating different cooperation incentive strategies. Here they are integrating price based and reputation based methods to stimulate security in autonomous Mobile Ad Hoc Networks under noise and attacks, and the damage that can be caused by attackers is bounded and limited. Though it limits the malicious behaviors of selfish nodes, it has their own disadvantages. They propose to integrate two different cooperation incentive strategies using a framework. Though the framework provides good support, due to the heavy load of incentive strategies, the system looks complex and sometimes takes lot of time in determining the trustworthy nodes.

III. PROPOSED SYSTEM

In our propose system, rather than integrating different incentive strategies, we focus on reputation based system alone and enhance it for the better identification and prevention of selfish nodes.

The main goal of this project is to detect the malicious nodes (Non co-operative nodes) in the network and avoid them to conserve computational resources such as power consumptions etc. And choose a trustworthy node in order to forward a packet in the network. We face problems while forwarding the packets in a single best path chosen as they are chance that the node in the path may drop the packets in order to retain its CPU resources. So our main goal is to efficiently increase the QOS factors like: Throughput, Delay and Security by using hybrid reputation system.

Secondly we provide essential security by using ERAODV that forwards the packet in a multi path manner, which provides security against the sniffing attacks on the network. So, by integrating both the hybrid system and the ERAODV, high throughput with security is achieved.

A. Reputation System

Reputation system is the main approach proposed to encourage cooperation between mobile nodes in MANETs. A reputation system gathers node behaviors and calculates node reputation values. The system detects and punishes low-reputed nodes by isolating them from the MANETs. There are two types of reputation systems: first hand based and second hand based.

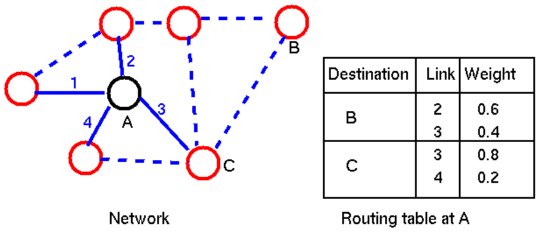
In first hand based reputation systems, a node only believes its own observations about others node’s behavior, and the exchanges of reputation information between nodes are disallowed. Let the source node choose the next hop node with sufficiently high reputation during the packet routing in order to achieve routing reliability. Second hand based reputation system avoids indirect reputation information and uses only direct observations in order to see the performance of this method. We propose to expand the scope of the behavior observation from one hop to two hops.

In the second-hand reputation systems, nodes share observations of node behaviors by periodically exchanging observed information. In core, a node promiscuously listens to the transmission of the next node in the path to detect misbehavior, and aggressively informs other nodes of the misbehaviors by reporting around the network to isolate the misbehaving nodes. Although observation sharing has some potential drawbacks such as increased transmission overhead, misreporting and collusion, it can detect node misbehavior faster than the first-hand-based reputation systems. Although these reputation systems use linear or nonlinear reputation adjustment mechanisms for reputation calculation, they still use a threshold to distinguish selfish nodes from cooperative nodes. Thus, clever selfish nodes can wisely maintain their reputation value just above the threshold by selectively forwarding others' packets regardless of the reputation calculation mechanism. Such nodes can take advantage of other cooperative nodes without being detected. Also, these methods cannot reward high reputed nodes differently or punish low-reputed nodes in different reputation levels.

B. Multipath Routing System

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multipath routing techniques, but multipath routing is not yet widely deployed in practice.

It is desirable to allow packets with the same source and destination to take more than one possible path. This facility can be used to overcome node failures and improve security. To operate such a scheme consistently nodes must maintain routing tables specifying what goes where. The mechanisms for this differ with datagram and virtual circuit transport.



Routing table at A

Destination	Link	Weight
B	2 3	0.6 0.4
C	3 4	0.8 0.2

Figure1: Multipath Routing

The network above has all the links to node A numbered, its datagram routing table is shown. The weights in the table represent the probability of the link being chosen for the destination specified. A random number will decide where the packet actually goes. The weights represent ratios of some metric of path length. All virtual circuit packets in a given conversation must take the same route. When a conversation's first packet arrives at a node, it allocates the conversation a virtual circuit number on a selected link and sets this on the virtual circuit routing table, as shown. It can be seen in the above diagram that the virtual circuit numbers varies from link to link for a specific conversation. This allows the numbers of virtual circuits on a given link to be set (in relation to capacity etc.) at set-up and subsequently allocated as required by the network system.

C. Enhanced Reverse Ad hoc On Demand Vector Routing Protocol (ERAODV)

Enhanced RAODV is our proposed protocol, which extends the Reverse AODV protocol. In Ad hoc networks, malicious nodes can enter in radio transmission range on the routing path and disrupt the network activity and also affect the performance of the whole network. Therefore, protecting the network from intrusion of malicious node and enhance data security is an important issue on Mobile Ad hoc networks. Enhanced RAODV provides a path hopping method based on reverse AODV (R-AODV). By Reverse AODV, source node builds a multipath to the destination and adaptively hops all available paths for data communications. Hopping paths can protect data from the intrusion of malicious nodes.

We integrate the Hybrid Reputation System, which identifies and avoids the non-cooperative and Packet forwarding system in Our Proposed System.

IV. CONCLUSIONS

A mobile Ad-hoc network provides the mobility of nodes which is so helpful in any emergency situations. However, if security accidents and packet loss occurs, ruinous economic damages are inevitable. Our proposed a new hybrid reputation system that focuses on detection on malicious node and avoids them to increase the Qos parameters. Proposed method provides how we decrease the traffic and rate of vulnerability in the system using ERAODV protocol.

REFERENCES

[1] A. Aram, C. Singh, S. and A. Kumar, (2009) “Cooperative Profit Sharing in Coalition Based Resource Allocation in Wireless Networks”, Proc IEEE INFOCOM.

[2] S.Bansal and M.Barker, “Observation based cooperation enforcement in Ad-Hoc networks”, Arxiv preprint cs/0307012, 2003

[3] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs,” IEEE Trans. Mobile Computing, vol. 6, May 2007.

[4] L.Anderegg and S.Eldenbenz, (2003) “AdHoc VCG: A truthful and cost efficient routing protocol for mobile adhoc Networks”, Proc ACM MobiCom

[5] S.Zhong, J.Cheng and Y.R.Yang ,”Sprite:A simple chat proof credit based system for mobile adhoc networks”, Proc IEEE INFOCOM, 2003.

[6] P.Dewan, P.Dasgupta and A.Bhattacharya , “On using reputations in adhoc networks to counter malicious nodes”, Proc. Int’l Conf.Parrallel and distributed systems (ICPADS), 2004

[7] M.T. Refaei, L.A.

[8] , M. Eltoweissy and T. Nadeem, (2010) “Adaption of Reputation Management Systems to Dynamic z Conditions in Ad Hoc Networks”, IEEE Trans.

[9] P.Michrardi and R.Molva, (2004) “CORE: A collaborative reputation mechanism to enforce node cooperation in Mobile adhoc networks”, Proc. [9] K.Liu, J.Deng, P.K. Varshney, K. Balakrishnan,“An Acknowledgment-Based proach for the Detection of Routing Misbehavior in MANETs,” IEEE Trans. Mobile Computing, 2007.

[10] Z. Li and H. Shen, (2011) “A Hierarchical Account-Aided Reputation Management System for Large-Scale MANETs”, Proc IEEE INFOCOM.

[11] Wei Yu, K.J. Ray Liu,“Game Theoretic Analysis of Cooperation Stimulation and Security in Autonomous Mobile Ad Hoc Networks”, 2007

[12] Ze Li and Haiying Shen “Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING.

[13] K.Balakrishnan, J.Deng and V.K.Varshney, (2005) “TWOACK:Preventing selfishness in Mobile adhoc networks”, Proc. IEEE Wireless Comm. And Networking Conf.(WCNC).