A Basic Technology of Cooperation in Mobile Ad Hoc Networks

Raju Barskar
Student Of M Tech (CSE)
MANIT, Bhopal (M.P) INDIA

Rajesh Wadhvani
Assistant Professor,
MANIT, Bhopal (M.P) INDIA

ABSTRACT
'Mobile Ad hoc Networks' (MANETs) properties present major vulnerabilities in security. Wireless ad hoc technology is demanding and continually growing. Its dynamics and flexibility allow the network to be easily set up without the requirement of a predetermined infrastructure. The advancement of the technology itself draws attentions from intruders as well as researchers and developers. In a multi-hop hop mobile ad hoc network (MANET), mobile belonging to the first category are either faulty and therefore nodes cooperate with each other without using any cannot follow a protocol, or are intentionally malicious and infrastructure such as access points or base stations. They try to attack the system. The problems created by these nodes nodes' mobility and fundamentally limited capacity of the need to be addressed at many layers, for example, using wireless medium, together with wireless transmission effects spread-spectrum encoding to avoid interference over the such as attenuation, multi-path propagation, and interference communication channel, using a reputation system to identify combine to pose significant challenges for security in the malicious system, and subsequently avoid or penalize MANETs. This kind of selfishness needs a comprehensive mechanism to cope with and we have planned to publish such mechanism in early future.

General Terms
Algorithms, Performance, Economics, Reliability, Security, Human Factors and Wireless Ad hoc networks.

Keywords
Mobile ad hoc network (MANET), security, wireless network, Cooperation, Reputation, Selfishness, Malice nodes.

1. INTRODUCTION
An ad hoc network is a group of wireless mobile nodes, in which nodes cooperate by forwarding packets for each other to allow communication beyond their direct wireless transmission range. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. A wireless ad hoc network is a collection of two or more mobile communication devices capable of handling traffic flow while the devices are on the move. Every node in the network has the capability to route messages from itself or from other nodes to their destinations without the assistance of any centralized network equipments (i.e. router). Hence, the network does not require any existing communication infrastructure to assist in its services. With the decentralized characteristic of a wireless ad hoc network, there is a major concern on its security issues since the security policies of the traditional wired network cannot be directly applied because it lacks of centralized equipment to coordinate filtering of suspicious packets. Hence, each ad hoc node has to provide a basic security policy (e.g. encryption) to prevent intrusions. Each mobile unit requires an independent distributed system or a de-centralized system to manage the events that may occur during operations. Ad-hoc networks [1] have been proposed to support scenarios where no wired infrastructure exists. They can be set up quickly where the existing infrastructure does not meet application requirements for reasons such as security, cost, or quality. Examples of applications for ad hoc networks range from military operations, emergency disaster relief to community networking and interaction between attendees at a meeting or students during a lecture. In Mobile Ad hoc Networks (MANET) each node has limited wireless transmission range, so the routing in MANETs depends on the cooperation of intermediate nodes.Mobile ad hoc networks are paradigms for mobile communication in which mobile nodes are dynamically and arbitrarily located in such a manner that communication between nodes does not rely on any underlying static network infrastructure [2]. The communication medium is broadcast and the nodes in a mobile ad hoc network are usually portable mobile devices with constrained resources, such as power, computation ability and storage capacity. Since no fixed infrastructure or centralized administration is available, these networks are self-organized and end-to-end communication may require routing information via several intermediate nodes. We can identify two types of uncooperative nodes: faulty or malicious and selfish. Faulty/malicious behavior refers to the broad class of misbehavior in which nodes are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Selfishness refers to noncooperation in certain network operations. In mobile ad hoc networks, the main threat from selfish nodes is dropping of packets (black hole), which may affect the performance of the network severely. Both Faulty/malicious nodes and selfish nodes are misbehaved nodes. To prevent misbehaviors in ad hoc networks is to provide incentives for delivering services for the network. Here, the system offers incentive to mobile nodes that accurately play their roles. All nodes in the transmission path are compensated as the task is fulfilled. This incentive is used as a credit or virtual money for paying the transmission cost to other node, so that mobile nodes are willing to attend to the transmissions. Zhong et.al. [9] developed Sprite (A Simple, Cheat-Proof, Credit-Based System) for mobile ad hoc networks based on the stimulation approach introduced by Buttyan and Hubaux [10]. The authors proposed an incentive system without a tamper-proof hardware installed

in each mobile node. Accordingly, the source node needs to pay for the cost of transmission. The cost is illustrated in the form of credit or virtual money. It needs to give its credit to the nodes along the route to the destination. Therefore, if the nodes along in the path want the compensation, they have to relay the messages sent from the source to the destination. The credits earned, in turns, can be used whenever the node desires to send its own messages to others.

2. THE PROBLEMS

An adversary has no need to cheat i.e., misbehave for accessing the wireless medium when no one else attempts to transmit. Therefore, in order to minimize the probability of detection, an attacker will choose legitimate over selfish behavior when the level of congestion in the network is low. The problem that we address in this paper is the availability of services in terminode networks. In civilian applications of ad-hoc networks, which we are exclusively concerned with in the Terminodes Project, availability is often considered to be the security issue of greatest relevance for users [4]. We concentrate on two aspects of availability in terminode networks.

1.1 Issues with Reputation Method

The reputation based schemes applied to mobile ad hoc networks may be different in implementation; they are all composed of essentially three different parts:
1. The calculation and update of reputation values
2. The detection of misbehavior
3. The reaction to uncooperative behavior

2.2 The unique characteristics of mobile ad hoc networks raise certain requirements for the security mechanism.

1). Security mechanisms for enforce cooperation in mobile ad hoc networks should be distributed and self-organized. Security mechanisms involving any centralized service may no longer be viable because mobile ad hoc networks are self-organized and they cannot rely on any central authorities or external management.
2). Due to the constraints in bandwidth, computer power, and battery power in mobile devices, mechanisms should not cause undue resource consumption so as to degrade the performance of the network. Thus, there is an application-special trade-of between security and functionality.
3).The dynamic topology of mobile ad hoc network requires that the security mechanisms be scalable and reliable.

3. VIRTUAL CURRENCY SCHEMES

Since forwarding a message will incur a cost (of energy and other resources) to a node, an uncooperative node will need an incentive in order to forward messages of other nodes. Virtual currency systems [4, 7, 9, 10, 11] use credit or micro payments to compensate for the service of a node. A node receives a virtual payment for forwarding the message of another node, and this payment is deducted from the sender (or the destination node). Two examples of such systems are: Nuglets [7, 9, 10, 11] and Sprite [4].

3.1 Nuglets

Buttyan and Hubaux introduced a virtual currency, called nuglets, and present a mechanism of charging/rewarding service usage/provision to stimulate cooperation in self-organized mobile ad hoc network [7, 9, 10, 11]. Two models were presented for using the nuglets: packet purse model, in which the source of the packet is charged and packet trade mode, in which the destination is charged. In the packet purse model, when sending the packet, the source loads it with a number of nuglets sufficient to reach the destination. Each intermediate node takes some nuglets for the forwarding service. In the packet trade model, packets are traded for nuglets by intermediate nodes. Each intermediary node \buys" the packet from the previous node for some nuglets and \sells" it to the next node for more nuglets. In this way, every intermediate node gains nuglets for forwarding and the total cost of forwarding the packet is paid by the destination node.
To implement either the packet purse model or the packet trade model, tamper-proof hardware is required at each node to prevent the node from illegitimately increasing its own nuglets and to ensure that the correct amount of nuglets is deducted or credited at each node. Mechanisms that use nuglets have some other problems.

3.2 Sprite

S. Zhong et al. proposed Sprite [4], a simple, cheat-proof, credit-based system for mobile ad hoc networks. Sprite uses credit to provide incentives for mobile nodes to cooperate and report actions honestly. The basic idea of their scheme is as follows: a Credit Clearance Service (CCS) is introduced to determine the charge and credit to each node involved in the transmission of a message. When a node receives a message, the node keeps a receipt of the message and later reports it to the CCS when the node has a fast connection with the CCS. Payments and charges are determined from a game theory perspective. In this scheme, the sender is charged, in order to prevent a denial-of-service attack to the destination by sending it a large amount of traffic. A node that has tried to forward a message is compensated, but the credit that a node receives depends on whether or not its forwarding action is successful. Forwarding is considered successful if and only if the next node on the path reports a valid receipt to the CCS. Modelling the submissions of receipts regarding a given message as a one-round game, the authors proved the correctness of the receipt submission system using game theory [5, 6].

4. DISCUSSION ON VIRTUAL CURRENCY SCHEMES

The basic problem with virtual currency schemes is they either depend on the use of tamper-proof hardware to monitor the increase or deduction of the virtual currency (as Nuglets does), or require a central server to determine the charge and credit to each node involved in the transmission of a message (as Sprite does). Both approaches may not be appropriate for truly mobile ad hoc network scenarios. Also, they suffer from the location privilege problem [3]. Nodes in different locations of the network will have different chances for earn virtual currency, which may not be fair for all nodes. Usually, nodes at the periphery of the network will have less chance to be rewarded

5.1 Selfishness Models of Nodes

Selfishness in mobile ad hoc network has a significant importance, since harms it causes can not be alleviated by general security mechanisms like symmetric and asymmetric cryptography. On the other hand, it is almost probable in such networks that nodes act selfishly when they have limited energy power i.e. each node try to consume its energy just when it needs to send its own packets. If a selfish node does not cooperate in any route discovery process, it is implicitly eliminated from network, because it will come in no source route of a packet. Effect of such selfishness is approximately equal to effect of eliminating all selfish nodes form the network and just lowering network density. So we assume that a selfish node acts the same in route discovery and packet forwarding according to probabilistic and nondeterministic selfishness models we introduced in the following sections.

5.2 Linear Selfishness Model

According to sensitivity of mobile nodes to their energy consumption, it is reasonable and logical to suppose probability of selfishness behavior as a function of node's energy level. If we define *Si* as probability of selfishness in behavior of node *i* (i.e. probability that node *i* drops a data packet), then a simple model can be declared as following linear function.

5.3 Detection of Misbehavior and Tracing Fault

In order for reputation values to be valid, nodes will need a reliable way of detecting good or bad behavior. CONFIDANT, CORE and OCEAN all rely on promiscuous observation for monitoring function operations. However, passive observation presents several weaknesses used within mobile ad hoc network, it might not detect a misbehaving node in the presence of [4]. To detect misbehavior in DSR, Buchegger and Le Boudec use a reputation system [3]. Every node calculates the reputation of every other node using its own first hand observations and second hand information obtained from others. The reputation of a node is used to determine whether countermeasures against the node are undertaken or not. A key aspect of the reputation system is how second hand information is used, in order to avoid false accusations [3]

5.4 Reaction to Uncooperative Behavior

If a node's reputation value drops below the threshold, Ru, then it is considered misbehaved and a WARNING message about the node is generated. Before the WARNING message is broadcasted to the neighborhood, it should be signed by m nodes, where m -1 is the upper bound of malicious nodes in a one-hop neighborhood. This ensures the trustworthiness of the WARNING message and is robust against false accusation. Once an uncooperative node has been identified, it is isolated and exclude from the network. Usually, neighbors of the uncooperative node refuse to forward any packets originated from the convicted node, depriving the network services. However, since the function of a mobile ad hoc network depends on all the participate nodes. Thus, an uncooperative node should be punished temporally and be given chance to behave normal again. OCEAN uses the \Second Chance Mechanism" to allow nodes previously considered misleading to become useful again [13]. It uses a timeout based approach where an uncooperative node is accepted by the network after a fixed period of observed inactivity. The rating of the node is not changed, so that it can quickly be detected if the misbehavior continues.

6. ATTACKS

Malicious nodes attack by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information so that the network is not able to provide service properly. Attacks like reducing the amount of routing information available to other nodes, failing to advertise certain routes or discarding routing packets or parts of routing packets are due to selfish behavior of a node. Misbehaving node model as defined in [9] has three types of selfish nodes depending upon their extent of non-cooperation in network operations. Selfish node of Type 1 forwards control packets but does not forward data packets and are saving a significant portion of its battery life by neglecting data packets. Selfish node of Type 2 uses energy only for its communication and neither forward controls neither packets nor data packets. Selfish node of Type 3 depends on energy level. Let E be initial maximum energy of node. When energy of the node falls within (E, T1) the node behaves properly and execute both routing functions and packet forwarding. When energy falls in (T1, T2), the node behaves like selfish node of Type 1 and thus disables data packet forwarding. If energy falls within (T2, 0) then node behaves like selfish node of Type 2. With in a limited time interval the node's energy is set back to the initial value. In our protocol, we aim at protecting the network against attacks by selfish nodes and malicious nodes exhibiting the following misbehavior:

6.1 Black hole Attack

An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets. The attracting packets involve advertising routes as low-cost [2]. In networking, black holes refer to places in the network where incoming traffic is dropped without informing the source that the data did not reach its intended recipient In Black hole Attacks a node uses the protocol and advertises itself as having the shortest path to the destination node where the packet is destined to.

6.2 Grey hole Attack

Grey Hole is a node that can switch from behaving correctly to behaving like a black hole. This is done to avoid detection. Some researchers discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to a Route Reply (RREP); only the destination is allowed to reply [3].

6.3 Wormhole Attack

In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire

packet to be received. An attacker can create a wormhole even for packets not addressed to itself, since it can hear them in wireless transmission and tunnel them to the attacker at the opposite end of the wormhole

6. AUTHENTICATION ISSUES

In the work we present in this paper, we assume that nodes do not spoof each other's identities, since this would allow misbehaving nodes to exploit the good reputation of neighboring cooperating nodes. Since in reality it is easy to spoof IP addresses and even MAC addresses, this would imply the use of a cryptographically secure authentication mechanism, perhaps as provided through a secure routing protocol. Unfortunately, we do not yet find a secure routing protocol that handles authentication in a manner that matches the spirit of OCEAN in being truly ad hoc and also manageably simple. Some secure routing protocols rely on pre assigned certificates from common certificate authorities to authenticate nodes [9], but it may not always be possible in truly ad hoc contexts for nodes to hold such pre-assigned certificates from authorities that all nodes will respect. Efforts to develop on-the-fly certificate authorities within the network [10] [12] appear either to be quite complex or to distinguish the role of certificate authority among a subset of nodes, which does not provide complete decentralization.

7. CONCLUSIONS & FUTURE WORK

In this research, we propose nondeterministic and probabilistic models of selfishness in mobile ad hoc networks which are dependent on node's instantaneous energy level. Since selfishness usually arise form node's interest in its survivability, these models seem to be tangible and completely probable. Applying these models to MANETs shows that in the presence of energy-based selfishness when density is high, network throughput degrades faster than when density is low. We also conclude that mobility has a strong effect on network performance and throughput degradation is much faster when mobility is high. Other result of our simulation is corresponding to effect of time on throughput. Unlike absolute selfishness, energy based selfishness models causes network throughput to gradually decrease over time. The results prove that we should design a mechanism for coping with selfishness that encourages nodes to cooperate and deprives selfish nodes of routing services. When nodes show energy-based selfishness, this mechanism should have additional and strong features. We have assumed that selfish nodes drop packets with probability one. Only honest nodes are generating packets. These two assumptions may be relieved and network behaviors can be studied in presence of probabilistic reputation updating mechanism. Selfish nodes can be set to drop packets with varying probabilities, rather than one only. Selfish nodes may generate traffic also. A solution better than this which further increase PDR may be found. The MANETS security issues foster new ideas and approaches as it has got potential widespread applications in military and civilian communications.

8 . REFERENCES

[1] Ram Ramanathan and Jason Redi, "A brief overview of Ad-hoc Networks: Challenges and Directions", IEEE Communications Magazine May 2002, pp. 20-22.

[2] E.M.Belding-Royer and C.K.Toh. A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Personal Communications Magazine, pages 46-55, April 1999.

[3] Yongwei Wang, Venkata C. Giruka, Mukesh Singhal, A Fair Distributed Solution for Selfish Nodes Problem in Wireless Ad Hoc Networks, Ad-Hoc, Mobile, and Wireless Networks: Third International Conference, ADHOC-NOW 2004, Vancouver, Canada, July 22-24, 2004. Proceedings Pages 211-224.

[4] Sheng Zhong, Jiang Chen, and Yang Richard Yang, Sprite: A simple, Cheatproof,Credit-based System for Mobile Ad hoc Networks, in Proceedings of IEEE Infocom '03, San Francisco, CA, April 2003.

[5] Pietro Michiardi, Re_k Molva, Game theoretic analysis of security in mobile ad hoc networks, Research Report RR-02-070, April 2002.

[6] Dave B. Johnson and David A. Maltz., "The dynamic source routing protocol for mobile ad hoc networks". Inter-net Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, October 1999.

[7] L. Zhou and Z. Haas, "Securing ad hoc networks". IEEE Network, 13(6):pp-24--30, November/December 1999.

[8] P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.

[9] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: owards routing security, fairness, and robustness in mobile ad hoc networks," in 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, 2002.

[10] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks," in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June 2002. [Online]. Available: ttp://lcawww.epfl.ch/Publications/LeBoudec/BucheggerL02.pdf

[11] A. Fasbender, D. Kesdogan, and O. Kubitz. Variable and scalable security: Protection of location information in mobile IP. In Proceedings of the 46th IEEE Vehicular Technology Conference, Atlanta, pages 963–967, 1996.

[12] Z. Haas. Securing ad hoc networks. In IEEE Network magazine, special issue on networking security, Vol. 13, No. 6, November/Dezember, pages 24–30, 1999.

[13] B. R. Smith, S. Murthy, and J. Garcia-Luna-Aceves. Securing distance-vector routing protocols. In Proceedings of Internet Society Symposium on Network and Distributed System Security, San Diego, CA, pages 85–92, February 1997.