Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme

Mieso K. Denko
Department of Computing and Information Science
University of Guelph, Guelph, Ontario, Canada, N1G 2W1

ABSTRACT

Mobile ad hoc networks (MANETs) are dynamic mobile networks that can be formed in the absence of any pre-existing communication infrastructure. In addition to node mobility, a MANET is characterized by limited resources such as bandwidth, battery power, and storage space. The underlying assumption in MANETs is that the intermediate nodes cooperate in forwarding packets. However, this assumption does not hold in commercial and emerging civilian applications. MANETs are vulnerable to Denial of Service (DoS) due to their salient characteristics. There is a need to provide an incentive mechanism that can provide cooperation among nodes in the network and improve overall network performance by reducing DoS attacks. In this paper, we propose a reputation-based incentive mechanism for detecting and preventing DoS attacks. DoS attacks committed by selfish and malicious nodes were investigated. Our scheme motivates nodes to cooperate and excludes them from the network only if they fail to do so. We evaluated the performance of our scheme using the packet delivery ratio, the routing and communication overhead, and misbehaving node detection in a discrete event-simulation environment. The results indicate that a reputation-based incentive mechanism can significantly reduce the effect of DoS attacks and improve performance in MANETs.

Keywords: Ad hoc networks, mobile networks, wireless communication, Denial of Services, DoS, security.

1. INTRODUCTION

A DoS attack [9] is any event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. They pose threats to larger websites such as Amazon and eBay. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network. DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. Networks and applications can be attacked by modifying routing information or changing system configuration, thereby directly attacking data integrity. DoS attack packets may use spoofed IP addresses, and can occur in different forms including buffer overflow, TCP SYN flooding, Smurf, or Viruses. For example, in TCP SYN flooding, an attacker sends multiple connection requests to a victim, exhausting all of the victim's resources and preventing use by legitimate users. The emergence of new low detection rate DoS attacks, such as low-rate TCP-targeted DoS attacks [8], brings new challenges to the network services.

In MANETs, nodes act as both routers and ordinary nodes. Due to dynamic network topology and lack of centralized infrastructure, network security has brought a new challenge to networking communities. Unlike traditional networks, MANETs are more vulnerable to DoS attacks due to limited resources that force nodes to be greedy in resource utilization. When there is no cooperation, activities of even a small number of nodes may significantly decrease the performance of the network. For example, a misbehaving node that discards any packets passing through it can result in repeated retransmissions, which in turn cause network congestions. Also, a wireless link does not provide the same protection for data transmissions as does its wired link counter part. Hence, any user or receiver within the transmissions range can eavesdrop or interfere with data packets or routing information. Battery power is another critical resource for mobile nodes. If the battery power has been used up due to malicious attacks such as the sleep deprivation attack, the victim will not be able to provide network services. Since all nodes can be mobile, changes in network connectivity and resource availability also expose a network to various attacks. This calls for detection and prevention of attacks in the network.

Some intrusion prevention measures, such as cryptograph and authentication, can reduce the threats against MANETs. However, these mechanisms either cause greater overhead and latency or cannot defend against malicious internal nodes. The deployment of a Public Key Infrastructure (PKI) requires certification authority, but such an entity must always be available. Most current research on MANET security focuses mainly on secure routing.

Enforcing cooperation among nodes is one of the strategies for tackling security and improving MANET performance. Popular web-based services such as Amazon and eBay use reputation rating systems for buyers and sellers to rate each other; however, this mechanism relies on a centralized server to store and manage data. In eBay's reputation system, buyers and sellers can rate each other after each service, and the overall reputation of a participant is computed as the sum of these ratings over a period of months. The central location that

This research was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant No. 046940.

provides reputation information is usually a server with high computational and storage capability.

Although MANETs are based on the fundamental assumption that the nodes will cooperate in providing services or sharing available resources, non-cooperation is a critical problem when deploying these networks for civilian applications. Lack of cooperation in MANETs can be a result of misbehaving nodes or lack of sufficient resources. Misbehaving nodes can either be malicious or selfish. Selfish nodes are nodes that participate in the network to maximize their own benefit by using network resources while saving their own resources. Malicious nodes directly attack a network by disrupting its normal operation. The absence of a trusted third party in ad hoc networks necessitates the development of protocols for collecting, storing, and distributing reputations. Enhancing cooperation among nodes in the network can help in detecting and mitigating DoS attacks caused by the misbehaving nodes.

In this paper, we consider both a DoS attack caused by a selfish node that drops packet and a wormhole attack caused by a malicious node. We propose a reputation-based incentive mechanism for encouraging nodes to cooperate both in resource utilization and preventing DoS attacks. The main contributions of this paper are: (a) We use a clustering architecture to reduce the reputation data management overhead and improve monitoring capability; (b) We use a probabilistic selection strategy among all qualifying nodes for service provisioning to avoid overloading; and (c) We maintain an adaptive weight-based reputation rating based on neighbour and cluster-level information to improve the efficiency and effectiveness of DoS attack detection and prevention.

The rest of this paper is organized as follows. Section 2 presents a classification of ad hoc networks and attack scenarios. Section 3 presents motivation and related work. Section 4 presents the description of the proposed reputation-based incentive scheme. Section 5 presents the DoS attack detection and prevention mechanisms. Section 6 presents the performance evaluation based on simulation experiments. Finally, Section 7 presents the conclusion and future work.

2. CLASSIFICATION OF MOBILE AD HOC NETWORKS AND ATTACK SCENARIOS

Based on the composition of nodes that form a network, ad hoc networks can be classified into two main categories, cooperative and non-cooperative. In the first category, cooperative, nodes form networks based on common goals to achieve certain objectives. Examples are networks that can be formed in emergency relief operations, collaborative data processing, military applications, entertainment, and conference sessions. In this scenario all members of the group have common objectives, and therefore they cooperate. In the second category, a network is formed to establish communication in civilian environments. There is no reason for mutual cooperation. While the nodes in a network used by the soldiers in a battlefield or disaster recovery area can be assumed to cooperate, there is no good reason to assume that networks formed by civilians with diverging goals and interests will cooperate. Such a network can be formed by a group of people who want to communicate by establishing a temporary networking environment. Each user's objective is usually to maximize his own benefit, and hence the network may suffer from misbehaving nodes that may want to save their own resources while using other nodes for packet forwarding. It seems appropriate to use a mechanism that encourages cooperation in non-cooperating networks to improve network performance.

Non-cooperation in MANETs occurs due to misbehaving nodes and lack of resources in non-misbehaving nodes. In the non-cooperation due to misbehaving nodes scenario, nodes fail to cooperate due either to malicious behaviour or selfishness to maximize their own benefits. In non-cooperating scenarios, a node may promise to forward a packet but fail to do so, or may not be willing to forward packets to save its resources. In both scenarios, network services can be degraded due to lack of cooperation among the nodes. We consider this type of non-cooperation in our study.

In the non-cooperation due to lack of resources scenario, nodes fail to cooperate due to lack of sufficient resources. This resource shortage may occur as a result of wireless network characteristics (limited memory, bandwidth, or energy) or environmental conditions (unreliable connectivity or network load). This category of non-cooperative behaviour is called reasonable non-cooperation. The main issue that requires attention here is load balancing, which is required to distribute the network load equally among the nodes.

DoS Attack Scenarios

The DoS attacks that target resources can be grouped into three broad scenarios. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighbourhoods and to overload the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighbourhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in MANETs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences.

The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbours that communicate, overloads the network, and results in performance degradations. Such attacks can be prevented based on the reputation information exchanged among the involved nodes or the cluster head.

We attempt to prevent both selfish and malicious nodes from degrading network performance by providing incentives to encourage cooperation and punishing nodes that do not cooperate.

3. STIMULATING COOPERATION TO DEFEND AGAINST DOS ATTACKS

Motivation

Non-cooperative nodes in MANETs can degrade network performance through security threats including DoS attacks. Stimulating cooperation is an important measure in defending against attacks generated by misbehaving nodes. Attacks can be either active or passive. Active attacks can modify data, disrupt network operation, or disable services, while passive attacks do not alter data but fail to cooperate in providing services such as routing and packet forwarding. Active attacks on network routing include flooding, modifying routing information, providing false route requests and replies, attracting unexpected traffic, hiding error messages, and fabricating false error messages. Passive attacks include packet dropping to conserve resources. These abnormal node behaviours result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput. The effect of DoS attacks on MANETs can be serious, and the prevention and detection of these attacks is more difficult than in their wired counterparts.

Like other networks, the security requirements in ad hoc networks include services such as availability, authentication, non-repudiation, confidentiality, integrity, and access control. The limited processing and storage capability, bandwidth, and battery power of mobile devices prevent the implementation of complex algorithms in tackling attacks against MANETs. Moreover, due to the absence of a central entity for security management, unreliable links, and frequent membership changes, attacks from internal nodes are difficult to detect or prevent using existing security mechanisms.

Due to the absence of a fixed infrastructure for key management, centralized monitoring is impossible in MANETs. Reputation-based incentives can help in establishing more cooperative behaviour among non-cooperative nodes. A suitable security management system in this environment is a distributed mechanism where each node maintains local information, thereby incurring lower communication and computation overhead. We use clustering architecture to provide a localized monitoring mechanism to detect malicious nodes and improve the scalability of the proposed mechanism.

Related Work

Recently proposed incentive mechanisms for enforcing cooperation among nodes can be classified into trade-based and trust-based mechanisms. Trade-based mechanisms assume market models for providing virtual currency incentives for motivating cooperation among nodes. In the trust-based models, trust is created and the service provider is stimulated by these trust values. Each scheme can be deployed in different application scenarios. The trade-based models are not applicable in cooperative networks where no financial incentives are needed to run the network. However, trust-based schemes can still be used to improve network performance.

In the trade-model proposed in [1], every device has a tamper-resistant security module, PKI to ensure authentication. This security module is used for account management. Two billing models that charge nodes as a function of number of hops messages have travelled were proposed. An ad hoc participation economy (APE) that uses a dedicated banker node to manage accounts was proposed in [2]. Unlike the tamper-resistant mechanism, the APE uses dedicated banker nodes for account management and also has facilities for converting virtual currency into real monetary units. Incentive mechanisms that uses a node as a transaction manager are not plausible in dynamic ad hoc networks since location tracking incurs additional overhead. A similar reputation-based mechanism known as a reputation participatory guarantee (RPG) was proposed [3]. This mechanism provides a network layer solution that detects selfish nodes without propagating reputation ratings in the network.

A trade-based model that relies on the accessibility of banker nodes was proposed in [4]. This model does not use any tamer-resistant hardware but instead uses credit-clearance services in a wireless overlay network. In [5], a reputation-based model that investigates the effect of misbehaviour on network performance was presented. It uses a watchdog for identifying misbehaving nodes and a pathrater for selecting routes that do not select misbehaving nodes. In [6], CONFIDANT, a reputation-based model that removes misbehaving nodes by propagating bad reputation through the network was proposed. In [7], a reputation based model that only propagates positive reputations among the nodes was proposed. Reputation computation involves the aggregation of three different types of information based on different levels of observations and services. This method of reputation computation incurs greater overhead than other proposed schemes.

Existing incentive mechanisms for enforcing cooperation can be classified into trade-based [1,2,4] and reputation-based [3,5,6,7]. While the former uses a payment-based incentive, the latter uses mutual ratings based on services provided among the nodes.

While extensive work has been carried out on confidentiality, integrity, and privacy attacks [14], the threat to network availability has received less attention. Availability is an important requirement for improving network performance. Existing studies on DoS attacks concentrate on the analysis of various attack scenarios targeting a specific layer [15], or propose a probing mechanism to detect misbehaving nodes that target a specific network layer function [17]. While using a probing mechanism can help in detecting DoS attacks, probing packets may introduce communication overhead in the larger network. Reputation rating coupled with localized probing mechanisms can alleviate this problem.

4. DESCRIPTION OF THE PROPOSED SCHEME

Defending Against DoS Attacks

The two main schemes used in handling DoS attacks are detection and prevention. Detection involves locating an attacker and taking appropriate actions. Monitoring nodes' activity or tracing an attacker can help in detecting a DoS attack source. Several tracing and monitoring mechanisms have been proposed in the literature, including core-based and edge-based monitoring and deterministic and probabilistic packet marking. [16]. The prevention mechanism thwarts DoS attacks before they are launched. It does so by identifying an attack packet and taking action before it reaches its intended target. Common mechanisms used on the Internet include ingress or egress filtering and route-based packet-filtering mechanisms.

Proposed Architecture

Existing schemes in MANETs use either a prevention-only mechanism or detection strategies to defend the network from attacks. A prevention-only measure cannot eliminate attacks in an ad hoc networking environment. Also, detection alone is not sufficient to thwart attacks. Hence we adopt a combination of detection and prevention measures in our proposal. When an attacker is mobile, mechanisms such as traceback can be effective in determining the attack path or attack generating domain, but inefficient in identifying the attacking host.

Introducing some form of penalty to non-cooperating nodes and giving incentives to cooperating nodes may improve performance and ensure security in MANETs. This requires designing suitable data management and security architecture. We propose a reputation-based scheme for motivating nodes in ad hoc networks to prevent both active and passive DoS attacks. Unlike [7], we investigate the effect of both selfish and malicious nodes. Unlike [5,6], we do not exclude misbehaving nodes; instead we first encourage them to cooperate before excluding them. A node which becomes indifferent to its reputation and continues to act maliciously can be excluded from the network. If nodes do not cooperate, their reputation gradually goes down and they are eventually eliminated from the network. To avoid discriminating against new incoming nodes in reputation building, the age of a node is taken into account.

The proposed mechanism involves cluster formation, reputation database construction and maintenance, and information exchange. For local reputation ratings, data can be obtained from neighbors or a cluster head while inter-cluster reputation data can be maintained at the cluster head. In this scheme attempts will be made to stimulate nodes to cooperate while monitoring will be conducted to detect misbehaving nodes. Such misbehaving nodes will then be identified and considered for integration or isolation to avoid DoS attacks.

Assumptions

We make the following assumptions for the proper operation of the proposed scheme: (a) Each mobile node and cluster head in the network has a unique ID and can join or leave the network freely. (b) Reputation data exchanged between nodes is correct and there is no collusion among nodes. (c) Initially, all nodes have equal computational and storage capability, although a node may have more resources than others during the communication process.

Clustering Architecture

Monitoring and preventing DoS attacks is difficult in highly dynamic, large ad hoc networks. Hence, it is necessary to divide these networks into small and manageable groups and implement security mechanisms in each group in a distributed manner. Clustering provides a distributed and scalable architecture for network monitoring, reputation data management, and topology control. Clustering architecture also provides a localized attack detection and prevention mechanism through continuous monitoring and information exchange. This localized and distributed feature also reduces storage and communication overhead, thereby optimizing network bandwidth utilization.

The type of clustering algorithm used determines the stability of clusters. We use a variation of the clustering algorithm proposed in [10] where the election of the cluster head (CH) is performed based on a randomized rotation to allow load balancing by circulating this role among all nodes in the network. Unlike the purely random scheme proposed in [10], however, we use an aggregate parameter, which includes the available energy and mobility information for cluster head election. A node is eligible to become a CH only if it possesses adequate resources, in terms of battery power and lower relative mobility [13].

In this clustering architecture a localized topology control algorithm is used within a cluster and a distributed topology control algorithm is used among clusters. In the clustering architecture, each cluster has a CH, multiple nodes, and gateways. Each node knows its neighbours and hello messages are used to maintain connectivity information. A CH is a node that is responsible for managing network content; it also allows inter-cluster communication.

In a cluster-based scheme, an ad hoc network is treated as a community and each node is a member that shares common resources. A cluster corresponds to a community. As a community member with a good reputation gains respect or rewards, he earns better services, while a member with a bad reputation is eventually excluded from the network based on feedback mechanisms.

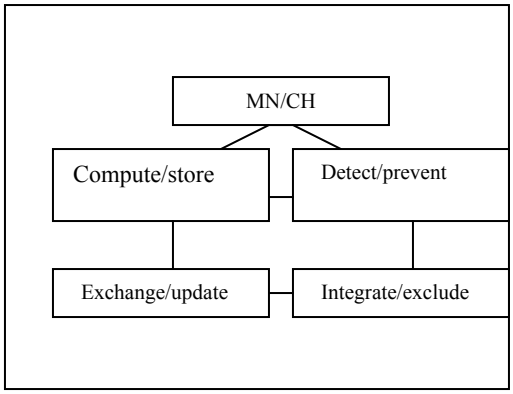

Figure 1: Data structure for reputation system

Reputation Management

One important issue related to reputation data management is deciding where to store the data and how to protect it from malicious node modification. Our proposed reputation system consists of four modules for reputation data management and decision making as shown in Figure 1. Mobile nodes (MN) and the CH compute and exchange reputation ratings. Using this information, a node can detect a misbehaving node and then integrate or it exclude from the network.

It is essential to aggregate local reputation data without a centralized storage and management facility. Possible options include aggregating the ratings of a few nodes (neighbours), the nodes in each cluster, or all nodes in a network. Maintaining all information at every node congests a network with system messages requiring each node to generate query or reply packets. We use a reputation system that aggregates the local reputation data of all nodes in a cluster. This provides a better scope than the neighbourhood only information and incurs minimum overhead as compared to global data maintenance.

There are three methods of reputation information exchange. the first is exchanging peer-to-peer information among the nodes. This means that information is maintained at each node and updates are sent to other nodes periodically. The second is obtaining information from other nodes through a discovery mechanism, and the third is relying on the CH for information gathering from each node. In this case, CHs periodically broadcast information upon receiving it from other nodes in the cluster. We use a combination of methods (a) and (c). Reputation data is collected and maintained at each node and the CH as discussed below.

Maintaining Reputation Data at Nodes: Nodes in each cluster monitor the behavior of their neighbors and update their reputation data periodically. Each node maintains information based on exchange of neighborhood and additional information obtained through a query-reply mechanism. Each node broadcasts its ratings periodically in a manner similar to a routing information exchange. Each node maintains a reputation database as a set of values *Nid*, *Scount* and *Ucount,* where Nid is the node ID, Scount is number of successful services, and Ucount is the number of unsuccessful services received from a node.

The reputation database is updated after each service by incrementing the suitable counter, according to observations or reports received from others. For example, each time node A gets service from node B, it rates the service as S(R(A,B) = 1) or U(R(A,B) = -1). Peer A may rate the service as negative if the service was not successful or denied but positive otherwise. Reputation data is computed as the sum of the ratings of the individual services. Each peer can store the number of satisfactory services it has had with peer B as S(A,B) and the number of unsatisfactory services it has had with peer B as U(A, B). For a node to be considered cooperative, its positive reputation rating should be at least equal to its negative reputation.

We use data query and reply messages which function as hello messages for the neighborhood communications. A node periodically updates reputation data. When a node joins the network, it is given a reputation value of 1. This reputation rating is called an initial threshold. The node's reputation data is updated based on the node's own observations as well as information received from peers both for data discovery and exchange mechanisms. Every time this rating is received, a new average is computed with more weight given to the node's own observation.

Maintaining Reputation Data by CHs: Reputation data is also maintained by CHs with information coming from nodes within the cluster or outside the cluster. The CH may periodically request reputation data from each member of its cluster and broadcast the result to all other nodes in the network. The aim of having the CH maintain reputation data is to propagate misbehaving node information as fast as possible to detect and prevent DoS attacks. Each cluster maintains a *global database* as a set of values (*Nid*, *Cid*, *Scount, Ucount*) associating with each Nid and Cid. The update strategy of the global database is achieved by incrementing or decrementing the appropriate counter. The arithmetic mean of reputation rating is computed at each service request and used for decision making.

Load Balancing for Cooperating Nodes
Each node normally forwards a packet via a node with a higher reputation rating. However, such a procedure may lead to overloading more cooperative nodes. Load balancing is one of the main issues that requires attention among cooperative nodes that willingly forward packets to others. Load balancing enables distribution of the network load equally among all potential forwarding nodes. We have used randomization as a means of distributing the load among nodes with higher reputation ratings.

We have implemented a probabilistic packet forwarding strategy among eligible nodes based on their reputation ratings. In this strategy, the forwarding task is accomplished probabilistically by choosing the next hop among all candidate nodes. This helps in balancing the load within the networks while overcoming the effect of packet dropping and selective forwarding. The basic steps for the load balancing procedure are: First, the source node selects a set (S) of nodes from its neighbors with reputation ratings above a threshold value;
Second, the source node sends a packet to a randomly selected node from the set S; The process then continues until the packet reaches its destination.

Weight-Based Reputation Updates
The proposed incentive mechanism was built on top of a clustering architecture where nodes in each cluster collaborate in the detection of selfish nodes. Forwarding packets originated from cooperative nodes and refusing those generated from selfish nodes can motivate cooperation. To increase the reliability of reputation rating and detect a malicious node that changes neighbours frequently, weighting was used while updating the reputation ratings. The process gives more weight to nodes' own observations and less weight to secondary information. Let R_o be a node's own observed reputation rating and R_n be neighbours' reputation ratings about the same node. Then, the updated reputation rating (R_u) is computed as follows:

$$R_u = \alpha R_o + \beta R_n \text{ , } \alpha, \beta \in [0,1], \alpha,>\beta.$$

Where α and β are configurable parameters and $\alpha+\beta =1$.

5. DOS ATTACKS DETECTION AND PREVENTION MECHANISMS

The Thread Model
We consider two types of DoS attacks. The first is packet dropping. This may involve dropping all received packets or selected packets. We characterize this as an attack generated by selfish nodes. A node is selfish if it drops messages to save its resources. The second type of attack is a wormhole attack. In this attack, a mobile node advertises a short routing path to its neighbours, tunnels the data and control packets it receives through the wormhole link, and replays them at the destination. Nodes that engage in this type of attack are called malicious nodes. A node is malicious if it misbehaves even if it loses its resources by doing so. False routes can be detected using reputation. For example, if a node advertises a short route and then drops or misdirects a packet, it can be considered a malicious node and its reputation rating can be reduced.

Dealing with Misbehaving Nodes
Nodes in each cluster collaborate in the detection of malicious nodes and the prevention of DoS attacks. This is achieved

through information exchange at various levels. For DoS attack management purposes, each node periodically performs the following operations:

1. Computes reputation ratings based on its own observations and second hand information obtained from neighbours and the CH. This is used to detect node misbehaviour. If the reputation falls below a predefined threshold, proceed to step 2.
2. Marks the node as selfish and broadcasts the new reputation rating to all neighbours and to the CH. All neighbours update their reputation information and decide the status of the node.
3. Periodically evaluates the reputation information of the node. Nodes are first warned and later excluded if they fail to cooperate in future communications. If they do cooperate, they are re-integrated. Their packet is not forwarded until their reputation rating reaches a threshold.

After detecting a misbehaving node, the information is used to prevent any further occurrence of DoS attacks by forwarding packets via other nodes. This can be achieved because each node maintains multiple routing paths based on reputation ratings. The reputation threshold values are dynamically selected and adaptive to the network condition as described in [12].

The system rewards nodes with high reputation ratings. For example, cooperating nodes are rewarded with prioritised services or greater bandwidths than non-reputable nodes. Thus, a packet sent by a node with a higher reputation rating gets higher priority in routing and experiences only minimum delay. We distinguish faulty nodes from misbehaving nodes by using a probing mechanism proposed in [13].

Parameters	Values/ranges
Simulation area	1000m x 1000m
Speed (m/s)	1 m/s to 20 m/s
Packet rate	5 packets /s
Packet size	128 bytes
Traffic source	CBR
Pause time	Uniformly distributed in 0-50 s
Routing protocol	AODV
Number of nodes (max)	100
Number of clusters	5-10
Transmission range	250m
Simulation time	900 s

Table 1: Simulation parameters

6. PERFORMANCE EVALUATION

Performance Metrics

The effects on performance of the fraction of misbehaving nodes, network size, pause time, and simulation time were investigated using the following four metrics:

1. Average packet delivery ratio. Defined as the ratio of the total number of data packets received by destinations and the total number of packets sent by a source.
2. Misbehaving node detection rate. Defined as the ratio of the total number of selfish nodes detected and the total number of selfish nodes in the network.
3. Routing and communication overhead. Defined as the ratio of the total number of routing and reputation-related packets and the total number of data packets.
4. Misbehaving nodes detection rate. Defined as the ratio of the total number of misbehaving nodes detected and the total number of misbehaving nodes in the network.

Simulation Environment

We carried out a performance evaluation using NS2 [11]. Nodes move according to the random waypoint mobility model [18]. The performance metrics monitored were packet delivery ratio, routing overhead, and misbehaving nodes detection rate. The effects of misbehaving nodes (selfish and malicious) on the performance metrics were investigated. The fraction of misbehaving nodes varied between 0% and 40%. Simulation parameters are shown in Table 1. Simulation results are shown in Figures 2-8.

Discussion of the Simulation Results

The simulation results that show the effect of the fraction of misbehaving nodes, network size, and mobility based on pause time are presented in this section.

The Effect of Misbehaving Nodes: Figure 2 shows the packet delivery ratio for misbehaving (selfish and malicious) nodes. The delivery ratio decreases with the increase in the fraction of misbehaving nodes with consistently better performance for the proposed scheme. The routing and communication overhead incurred is shown in Figure 3. The results indicate that the overhead slightly increases when the fraction of misbehaving nodes increases. The overhead incurred was mainly due to the transmission and retransmission of route discovery packets and reputation data exchange.

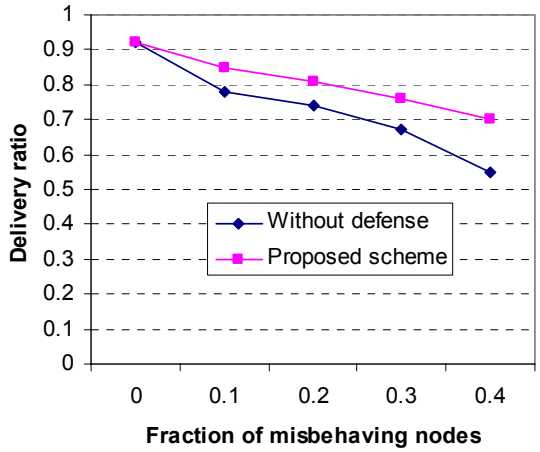

Figure 2: Delivery ratio as a function of misbehaving nodes

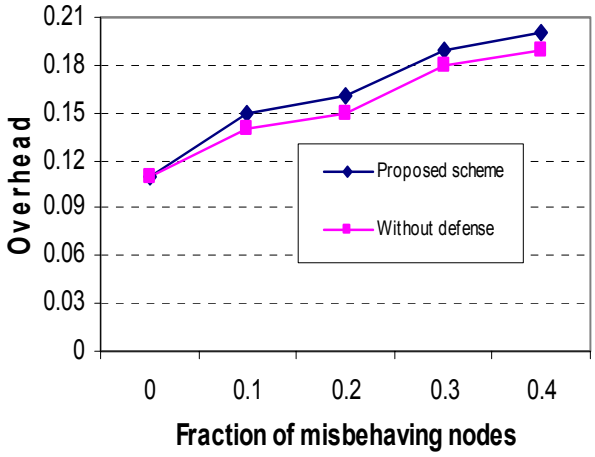

Figure 3: Overhead as a function of misbehaving node

The Effect of Network Size: The effect of misbehaving nodes as a function of network size was investigated, and the results are shown in Figure 4. The results show that the overhead incurred is low due to the use of clustering architecture. We also investigated the effect of network size on packet delivery ratio. The results in Figure 5 show that the packet delivery ratio slightly decreases, but that the proposed scheme outperforms the defenseless system. Compared with Figure 2, the increase in network size seems to slightly reduce the effect of misbehaving nodes. The result also suggests that the reputation-based incentive scheme coupled with load balancing is effective in detecting and preventing the DoS attacks caused by misbehaving nodes in ad hoc networks.

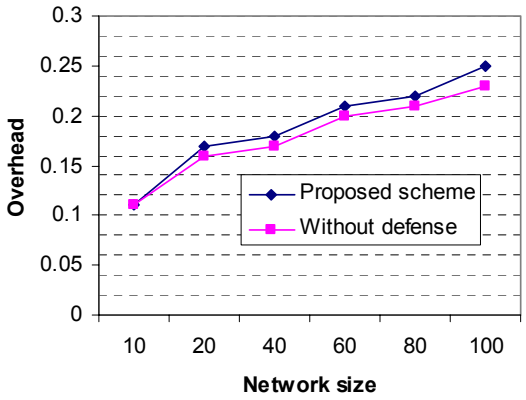

Figure 4: Routing and communication overhead as a function of network size

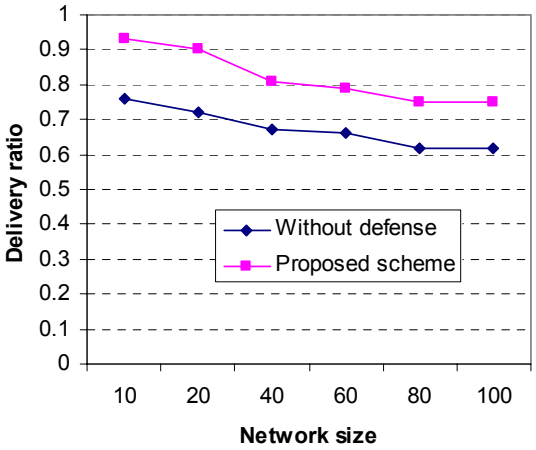

Figure 5: Packet delivery ratio as a function of network size

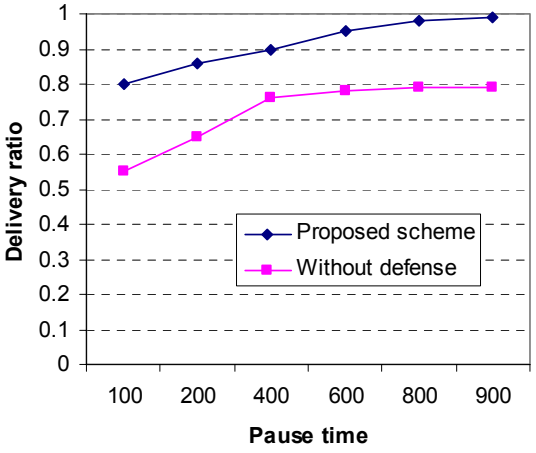

Figure 6: Delivery ratio as a function of pause time

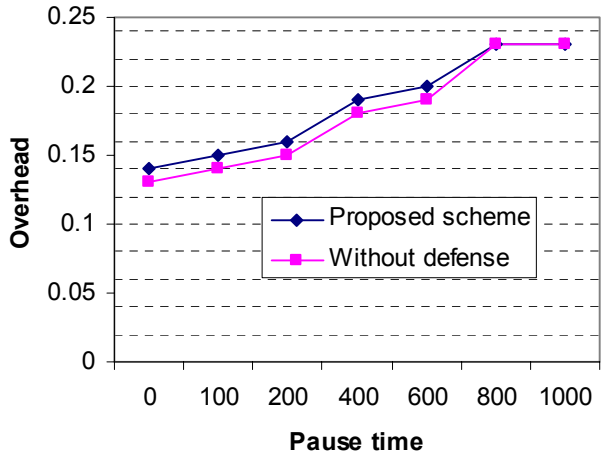

Figure 7: Overhead as a function of pause time

The Effect of Mobility: The simulation results in Figure 6 show that the packet delivery ratio increases as pause time increases and outperforms the defenceless network. This is

because low mobility allows longer connection time and more stable routing paths. However, even with perfect defence and static nodes it is not possible to achieve 100% packet delivery due to the unreliable links in wireless networks. Thus, the delivery ratio ranges between 80% and 99% for the proposed scheme.

The results in Figure 7 show that routing overhead for the proposed scheme is slightly higher than that for the defenceless network. This is at the cost of increasing cooperation, which increases the packet delivery ratio. The overhead was introduced due to frequent route maintenance, the exchange of reputation data, and route query and reply. The overhead ranges between 14% and 25%.

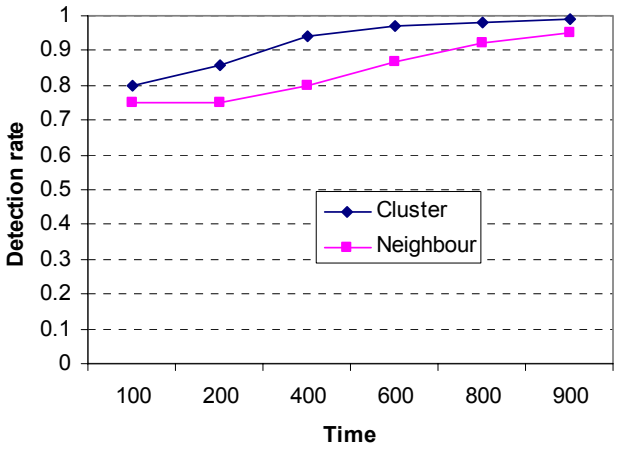

Figure 8: Detecting misbehaving node rate as a function of time

Misbehaving Nodes Detection Rate: This experiment was carried out to determine how long it takes to detect misbehaving nodes using neighbour and cluster-level reputation ratings. Cluster-level reputation rating refers to combined neighbour and cluster-level reputation ratings, while neighbour-level reputation refers to a reputation rating based on only neighbour information.

The simulation results in Figure 8 show that the detection rate of selfish nodes increases from 80% to 99% with cluster-level reputation information and from 76% to 97% with neighbour-level reputation information. The results show that when aggregated reputation information is used, the probability of detecting selfish nodes faster increases. This is because these nodes can be neighbours with at least one node and can easily be detected even when mobile. However, as the simulation time increases, the detection rates for both scenarios levels off.

7. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a reputation-based incentive mechanism for detecting and preventing DoS attacks in MANETs. A clustering architecture was proposed for performing reputation data management in a localized and distributed manner. DoS attacks were detected through collaborative monitoring and information exchange. Reputation rating was carried out using neighbourhood and cluster level information with more weight given to a node's own observation. A load balancing mechanism was used to reduce traffic on heavily used cooperative nodes. In this mechanism, selections are made probabilistically among the eligible nodes that are on the path to the destination.

We used the simulation technique to evaluate network performance in the presence of misbehaving nodes. Our simulation results indicated that the reputation-based incentive mechanism is effective in tackling DoS attacks that occur due to selfish and malicious nodes. The misbehaving node detection rate was higher when the aggregated reputation rating, as opposed to just neighbourhood information, was used. Future work includes the investigation of Distributed Denial of Services (DDoS) in MANET and integrated wireless networks.

REFERENCES

[1] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).

[2] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks," http://www.stanford.edu/~yl31/adhoc (2001).

[3] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks," http://www.stanford.edu/~yl314/adhoc (2002).

[4] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," Technical Report 1235, Department of Computer Science, Yale University (2002).

[5].S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In: Mobile Computing and Networking. (2000) 255–265.

[6] S. Buchegger and J.Y.L Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Noes — Fairness In Distributed Ad-hoc NeTworks," In Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, IEEE (2002) 226–236.

[7] P. Michiardi and R. Molva, "Making greed work in mobile ad hoc networks," Technical report, Institut Eur´ecom (2002).

[8] A. Kuzmanovic and E.W. Knight, "Low-Rate TCP-Targeted Denial of Service Attacks," SIGCOMM'03, August 25-29, 2003.

[9] A.D. wood and J.A. Stankovic, "Denial of Service in Sensor Networks," IEEE October 2002.

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless micro-sensor networks", In Proc. of IEEE Hawaii Int. Conf. on System Sciences, pages 4-7, January 2000.

[11] S. McCanne and S.Floyd,, Network Simulator. Http://www.mash.cs.berkeley.edu/ns/.

[12] M.K. Denko, "An Incentive-Based Service Differentiation in Mobile Ad Hoc Networks", In Proc. IEEE International conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005), pp. 197-204, August 2005, Montreal, Canada.

[13] M.K. Denko, "A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks", In Proc. IFIP INTELLCOMM'05, Montreal, Canada.

[14] I. Aad, J.P, Hubaux, and E.W. Knightly, “Denial of Service Resilience in Ad Hoc Networks”, ACM MOBICOM 2004, Philadelphia, PA, USA.
[15] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks. In Proc. of MILCOM, 2002.
[16] A. Habib, M. H. Hafeeda, and B. Bhargava, “Detecting Service Violation and DoS Attacks”, In Proc. of Network and Distributed System Security Symposium (NDSS), 2003.
[17] M. Just, E. Kranakis, and T. Wan, “Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks”, In Proc. of ADHOCNOW'03, Montreal, Canada.
[18] J. Broch, D. Maltz, and D. Johnson, “Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks”, In Proc. of IEEE Workshop on Mobile Computing, June 1999.