Computers **2015**, *4*, 87-112; doi:10.3390/computers4020087

OPEN ACCESS

computers

ISSN 2073-431X

www.mdpi.com/journal/computers

Article

A Dynamic Reputation Management System for Mobile *Ad Hoc* Networks [†]

Eric Chiejina *, Hannan Xiao and Bruce Christianson

School of Computer Science, University of Hertfordshire, College Lane, Hatfield, Hertfordshire
AL10 9AB, UK; E-Mails: h.xiao@herts.ac.uk (H.X.); b.christianson@herts.ac.uk (B.C.)

[†] This paper is an extended version of our paper published in the 6th Computer Science and Electronic Engineering Conference (CEEC), 2014, pp. 133–138. IEEE, 2014.

* Author to whom correspondence should be addressed; E-Mail: e.chiejina@herts.ac.uk;
Tel.: +44-1707-281093 ; Fax: +44-1707-284303.

Academic Editors: Laith Al-Jobouri and Mohammed Rashid Al-Mulla

Received: 30 January 2015 / Accepted: 14 April 2015 / Published: 17 April 2015

Abstract: Nodes in mobile *ad hoc* networks (MANETs) are mandated to utilize their limited energy resources in forwarding routing control and data packets for other nodes. Since a MANET lacks a centralized administration and control, a node may decide to act selfishly, either by refusing to respond to route requests from other nodes or deceitfully by responding to some route requests, but dropping the corresponding data packets that are presented for forwarding. A significant increase in the presence of these misbehaving nodes in a MANET can subsequently degrade network performance. In this paper, we propose a dynamic reputation management system for detecting and isolating misbehaving nodes in MANETs. Our model employs a novel direct monitoring technique to evaluate the reputation of a node in the network, which ensures that nodes that expend their energy in transmitting data and routing control packets for others are allowed to carry out their network activities while the misbehaving nodes are detected and isolated from the network. Simulation results show that our model is effective at curbing and mitigating the effects of misbehaving nodes in the network.

Keywords: selfish nodes; deceitful nodes; direct monitoring; total reputation; reputation management; MANETs

1. Introduction

Mobile *ad hoc* networks (MANETs) are vital to the advancement of wireless networks. MANETs are characteristically composed of equal nodes that communicate over wireless links without any backbone. Some applications, such as strategic military communication, rescue missions in times of natural disasters and sensor networks, are just a few possible uses of MANETs [1]. The emergence of the MANET technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, advance to autonomous networks. In either case, the propagation of MANET-based applications depends on a multitude of factors [2].

MANETs generally inherit the conventional problems of wireless and mobile communications. These include issues related to bandwidth optimization, power control and transmission quality enhancement [1,3]. In addition, the multi-hop nature and absence of fixed infrastructure generate new problems, such as configuration advertising, discovery, maintenance, as well as *ad hoc* addressing and self-routing. MANET topology is highly dynamic and random. Furthermore, the distribution of nodes and their ability to self-organize play an important role. Aside from their dynamic topology, due to their wireless transmission, MANETs are affected more by higher loss rates, higher delays and jitter than fixed networks. In addition, nodes in MANETs rely on batteries or other exhaustible power supplies for their energy. The most critical aspect of a MANET is that physical security is limited due to wireless transmission [1–5].

Security in MANETs mainly involves confidentiality and integrity of information, as well as legitimate use and availability of service [6]. Due to some characteristic features, MANETs are vulnerable to various security threats, such as eavesdropping, denial of service attacks (DoS), grey-hole attacks, black-hole attacks, *etc*. [4]. In a grey-hole attack [7,8], the malicious node behaves correctly by sending valid route replies to nodes that initiate route requests. If the malicious node is chosen as the nearest node to the required destination, it periodically drops the data packet to launch a DoS [8–10] attack. In the case of a black hole attack [11], the malicious node waits for neighbouring nodes to send route request messages. It replies to the request by providing a route to the destination over itself. It assigns a high sequence number in the reply message, which enables it to be seen as the best route to the required destination. By taking over all of the route, the malicious node discards all of the packets passing through it, by launching a DoS attack [9,11].

The existence of well-known intrusion prevention mechanisms, such as cryptography or authentication, can reduce threats against MANETs, such as malicious data modification, which aims to reduce data integrity and confidentiality [12]. However, they cannot defend against malicious internal nodes that disrupt the routing of data. Furthermore, conventional cryptography and authentication mechanisms cannot effectively address the above-mentioned threats that arise due to the inherent broadcast wireless medium and decentralized architecture of MANETs.

In general, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. Particularly in MANETs, any node may compromise the routing protocol functionality through a disruption of the route discovery process [2]. In order to ensure the availability of data in a MANET, all nodes in a MANET must act as routers for forwarding data packets from the source to the desired destinations [5]. It is therefore important for all nodes in a MANET to collaborate for the effective and efficient operations of the network.

However, due to the limited network resources and energy-constrained nature of nodes, it is expected that some nodes will exhibit uncooperative behaviours. These behaviours may adversely affect the overall network performance and put a further strain on the limited energy of the cooperative nodes. Specialised protocols have been employed in the network layer of nodes in MANETs to ensure collaboration among nodes. It is usually expected that these nodes will carry out their operations in compliance with the protocol specifications. However, these expectations are not always met.

Nodes sometimes make local decisions on whether to follow the network's basic operations or not. These nodes may decide to act selfishly by not participating in route discovery processes or deceitfully by responding to some route requests, but ensuring that the corresponding data packets are dropped. These misbehaving nodes specialise in conserving their limited energy resources, while the good nodes consume their own energy to ensure that the network is operational. An increase in the number of nodes exhibiting these types of behaviours may result in reduced network efficiency.

Countermeasures for node misbehaviour and selfishness are mandatory requirements in MANETs. Selfishness that causes a lack of node activity cannot be solved using classical security means that aim at verifying the correctness and integrity of an operation. It is therefore essential to employ a management system that will ensure an effective and reliable collaboration of all nodes in a MANET. An effective reputation management system would ensure that a node attains a certain reputation level before it can effectively operate in a network. This would ensure a gradual reduction or elimination of misbehaving nodes trying to disrupt the operations of the network [13].

In this paper, we propose a novel approach in monitoring the packet transmission activities of mobile nodes. The reputation of nodes is evaluated using a data-driven weighted average approach, which is based on the number of successfully transmitted data and control packets that a node carries out for other nodes as against its own transmitted packets. The distinctive direct monitoring approach employed in the proposed dynamic reputation management system is effective at detecting and mitigating various misbehaviours exhibited by nodes in a MANET. The use of directly obtained information to evaluate the reputation of nodes ensures that nodes do not rely on second-hand information before evaluating the reputation of its neighbours. This eliminates the possibility of obtaining false second-hand information, which can be used to carry out attacks, such as bad-mouthing and ballot-stuffing, as described in [14–17]. Furthermore, the reliance on directly obtained information will help in reducing routing overhead and in decreasing additional energy requirements.

The rest of the paper is organised as follows: Section 2 contains related works on trust and reputation management systems in MANETs. Section 3 discusses issues concerning misbehaving nodes in MANETs. Section 4 presents the proposed dynamic reputation management system. Section 5 presents details of the implementation work. Section 6 presents the simulation results and analysis. Section 7 concludes by setting out the benefits of the proposed system and outlines future research works.

2. Related Work

Cooperation enforcement in MANETs using the concept of reputation management systems has received considerable attention by researchers in the *ad hoc* network community. Over the past decade, a lot of research works have been proposed and carried out on trust and reputation management (TRM) systems in MANETs, which employed price-based and reputation-based schemes to enforce cooperation among nodes in the network. The price-based schemes [18–23] treat packet forwarding as a service that can be paid for and, thus, introduce a form of virtual currency to regulate packet-forwarding collaboration among nodes. Most of the price-based schemes require tamperproof hardware [18,19] or virtual banks that all of the nodes in the network can trust [20,21]. These price-based schemes use the virtual currency as a form of reward to nodes that participate in packet forwarding activities. In cases where a trust authority or virtual bank is required, it requires assistance from a fixed communication infrastructure to implement the reward schemes, which is not applicable for a pure *ad hoc* network [24].

On the other hand, reputation-based schemes [7,25–37] employ different monitoring techniques in gathering data, which are used in computing the reputation and trust of nodes in the networks [24]. A significant number of publications have proposed various reputation management-based techniques in which nodes in a MANET monitor the packet forwarding activities of their neighbours. If a node contributes in forwarding packets, the reputation of the node is increased. On the other hand, there is a decrease in the reputation of a node if it discards packets by dropping it. Subsequently, if a node's reputation drops below a certain threshold, the node is either punished or isolated from the network [3]. Several proposed TRM systems rely on first-hand and second-hand reputation information before computing the aggregated reputation of a node in their network. The second-hand reputation is obtained from their neighbouring nodes, while the data used in computing the first-hand reputation of nodes are derived using the watchdog mechanisms, as seen in several research works that are presented below.

Marti *et al.* [7] proposed a reputation-based technique that employs a watchdog and path rater. Each node in their model employs the watchdog to overhear packet transmission and checks if the next-hop node forwards the packet or not. The watchdog mechanism is based on promiscuously listening to packet transmission emanating from the neighbouring node. A monitoring node maintains a buffer of recently sent packets and compares each overheard packet with the packet in the buffer to determine whether there is a match. If a match exists, the packet is removed from the buffer, and the node is determined to be a normal node. However, if a packet stays in the buffer for longer than the expected period and no transmission is overheard, a failure count is incremented. If the count exceeds a certain threshold value, it determines that the node is misbehaving, and the source node is notified.

Buchegger and Boudec [31] modelled reputation system for MANETs using a protocol known as CONFIDANT (cooperation of nodes: fairness in dynamic *ad hoc* networks). The protocol specialises in the detection and isolation of nodes exhibiting anomalies in the network. The CONFIDANT protocol employs a monitoring system for observations. This includes a reputation system that specialises in knowledge creation based on first-hand and second-hand observations, a trust manager that manages incoming and outgoing second-hand reports from neighbouring nodes and a path manager that implements routing decisions through the elimination of paths containing misbehaving nodes and re-ranking of the other path based on the reputation of the nodes on the paths. Furthermore, CONFIDANT also utilises a passive acknowledgement scheme. This scheme confirms when the next-hop node in a routing path has forwarded a data packet. Although CONFIDANT ensures that low ranking nodes are denied data forwarding services, the monitoring scheme employed in the protocol will not be able to detect selfish nodes that do not participate in route discovery processes, because these nodes will never be presented packets for forwarding.

He *et al.* [29] proposed a secure and objective reputation-based incentive scheme for MANETs. The reputation of nodes in their proposed model is quantified by objective measures, and the propagation of reputation is efficiently secured by a one-way hash chain-based authentication scheme, which is computationally efficient and eliminates the need for a public key infrastructure (PKI) or other forms of authentication infrastructures. Their model uses punishment as a way of encouraging packet forwarding and disciplines selfish nodes by probabilistically dropping packets that originate from those nodes.

In [38], the authors proposed a trust management system (TMS), which includes a reputation system and a watchdog. Watchdogs normally monitor the events of data forwarding and count the arrival of the acknowledgement packets (ACKs) with respect to the forwarded data. The watchdog in their model employs a positive feedback message (PFM) as the evidence of the forwarding behaviour of a node. The trust evaluation in their model is a combination of both direct and indirect observation of nodes activities. Their model aimed at detecting malicious nodes' attempts to degrade the network performance through dropping or arbitrarily forwarding data.

Banerjee *et al.* [8] proposed a reputation-based trust management system for detecting and preventing vulnerabilities in MANETs. In their model, the node evaluates and exchanges the reputation values with its one-hop neighbours in the form of trust vectors. Trust vectors in their system signify the outcomes of previous transactions, and it is preserved for each neighbour that it had transactions with in the past. Every time a node intends to forward a packet, it checks the trust rating of the nodes connected downstream from its routing table. If the node is trusted, the packet is then forwarded. On the other hand, if the node is not trusted, a different downstream node is chosen randomly among the trusted nodes. Their proposed scheme works in a purely distributed manner, whereby attacks are detected by collaborative monitoring and information exchange among the nodes. The monitoring scheme employed in their model requires a node to monitor its upstream node, and trust computation is based on the received acknowledgement from the node.

Gupta and Kumar [39] proposed a novel routing strategy that deals with nodes that, due to loss of power, become selfish after previously being classified as trustworthy. Their strategy assumes that the selfish nodes are not malicious in nature, thus ensuring that they are mandated to provide accurate information about their current energy level. The information containing the status of a node's energy level is exchanged through periodic updates with its neighbours. The knowledge about the power status of the neighbours helps a node to avoid those nodes with very low power. This is based on the assumption that a node with low energy level may drop the packets presented to it for forwarding in a selfish manner in order to save energy.

Gong *et al.* [40,41] emphasized the importance of identifying selfish and malicious nodes to enable proper functioning of a MANET. They carried out critical reviews of some existing secure routing techniques and proposed an approach that incorporates a trust vector model within existing routing protocols. In their proposed model, each node monitors the traffic of its neighbours and evaluates its local trust vector about its neighbours. The nodes in their model monitor the packet forwarding activities using promiscuous listening of traffic. When a node overhears its immediate neighbour node forwarding a packet, it first checks the integrity of the packet in order to ensure that the packet had not been modified. If the neighbour being monitored passes the integrity test and the packet is forwarded, its trust vector is computed. Performance evaluation of their system shows that their mechanism successfully detected malicious nodes and avoided them in the routing path.

Bakar and Irvine [42] proposed a new mechanism to detect selfish nodes, which specializes in dropping control packets to avoid them being asked to forward data packets. Each node in their model operates in promiscuous mode to monitor both data and control packets that are transmitted within its receiving range. The monitoring node stores successfully observed transactions carried out by its neighbouring nodes. Nodes in their proposed model are expected to contribute to the network within a time frame. Those that fail to contribute to the network activities will undergo a test for their suspicious behaviours. Performance evaluation shows that their scheme was able to detect selfish nodes in a network.

In [43], the authors proposed a 2ACK scheme, which focuses on detecting misbehaving links instead of misbehaving nodes to avoid several issues, such as ambiguous collisions, receiver collisions and limited transmission power, which affect the general watchdog detection mechanism. The 2ACK scheme detects misbehaviour through the use of a new type of acknowledgement packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. When a node wishes to communicate with another node, a methodology is performed by the sending and receiving nodes, which ensures authentication and integrity. Security in their model is achieved through the use of cryptographic algorithms.

Ayday and Fekri [17] proposed a belief propagation-based trust and reputation management for P2P networks, which can also be utilized by social and mesh networks. In their proposed algorithm, the reputation and trustworthiness of a network node is computed by the Belief Propagation-based distributed message passing algorithm between peers (network nodes), which is presented on a chosen factor graph. The reputation of peers is based on the quality of service a node receives, and trustworthiness is based on the ratings that each node provides after successful transactions. Performance evaluation of their proposed model shows that it iteratively decreases the error in the reputation values of peers due to the malicious ratings with a high probability.

Further works were carried out by Ayday and Fekri [16] in which they proposed a trust management and adversary detection scheme for delay-tolerant networks (DTNs). Their proposed scheme was further extended in [15], which comprises a comparison of their proposed model with some well-known and commonly-used reputation management techniques (e.g., EigenTrust and Bayesian framework). The evaluation in their work shows the preeminence of their proposed scheme in terms of robustness against malicious behaviour. The performance evaluation described in [15,16] shows that their proposed model provided high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks. These attacks attempted to both undermine the trust and detection scheme and the packet delivery protocol employed in their proposed model. In particular, their proposed model was very effective and efficient at curbing Byzantine attacks in which one or more genuine nodes have been compromised. Despite relying on second-hand reputations from other nodes, their proposed model was able to mitigate the effects of bad mouthing and ballot stuffing attacks. However, one form of attack that may go undetected when employing this scheme is the selective existence attack carried out by totally selfish nodes. The nature of these nodes means that they will not participate in route discovery processes for other nodes. Thus, these nodes will never be presented data packets for forwarding. This type of node can never act as a service provider in a MANET, making it difficult for existing watchdog mechanisms that rely on feedback to compute the direct reputation of nodes.

When we compared some of the above-mentioned related works to our proposed model, one significant difference is in the monitoring technique that we employ in detecting misbehaving nodes. For instance, the watchdog monitoring techniques employed in [7,8,29,31,38–42,44] have the ability to detect when a node forwards a packet by listening to the traffic of the forwarding node. When it overhears the packet being forwarded, it uses the information to compute the corresponding reputation or trust values. Although, the watchdog mechanism is effective at detecting successful packet dropping and forwarding activities of nodes in MANETs, the watchdog mechanism has its own limitations. The watchdog mechanism is prone to ambiguous collisions, receiver collisions and limited transmission power, which may lead to false detection. More significantly, the watchdog monitoring technique will not be able to monitor and detect the network activities of selfish nodes that do not participate in the route discovery processes for other nodes. Nodes exhibiting this type of selfish behaviour will not be presented packets to forward for other nodes, which ensures that they will not act as service providers for other nodes in the network. However, the limitation of the watchdog mechanism in reference to monitoring the network activities of nodes exhibiting totally selfish behaviours is addressed by the monitoring scheme employed in this work. In our proposed work, a node relies only on first-hand information in computing the reputation of its neighbours. It captures packets through promiscuous listening of transmissions carried out by all of its neighbours and on packets it received from the target nodes that are being monitored. It employs a novel technique to analyse and filter each received and captured packet to identify if the node being monitored is the originator or just a forwarder. A full description of the monitoring technique is described in Section 4.1.

3. Threat Model

MANETs generally suffer from several vulnerabilities, which are exploited by misbehaving nodes in the networks. Some of these exploitations occur at the routing layer, and the resulting attacks are mostly carried out by these misbehaving nodes operating inside the network. Some of these attacks are explained below.

3.1. Selective Existence (Totally Selfish Behaviour)

A misbehaving node is said to exhibit a totally selfish behaviour if it does not participate in network operations, but uses the network for its advantage to enhance its performance and save its own resources, such as energy. This selfish node only makes its presence known to other nodes in the network whenever it wants to send its own packets. These selfish behaviours are known as selective existence attacks [3]. When a selfish node wants to send its own packet to another node, it performs a route discovery and then sends the required packets. When the node no longer needs to use the network, it returns to the silent mode. It ensures that all control packets that are presented during route discovery requests by other nodes are dropped. After a given period, its neighbouring nodes update their various route entries and delete their entries with routes with the destination to this node; this makes the node invisible to the network. Employing the passive acknowledgement mechanism used by some of the existing TRM systems mentioned in Section 2 will not be able to detect these totally selfish behaviours.

For instance, Figure 1 shows a MANET with nine nodes consisting of various paths from a source to a destination. If Node 1 wants to send a packet to Node 9, there are several possible paths to the destination assuming that all of the nodes are cooperative. If Node 4 and Node 6 were non-cooperative nodes exhibiting totally selfish behaviours, this means that all data from Node 1 must go through Node 3 (1-3-5-8-9) or through Node 5 (1-5-8-9), as seen in Figure 2.

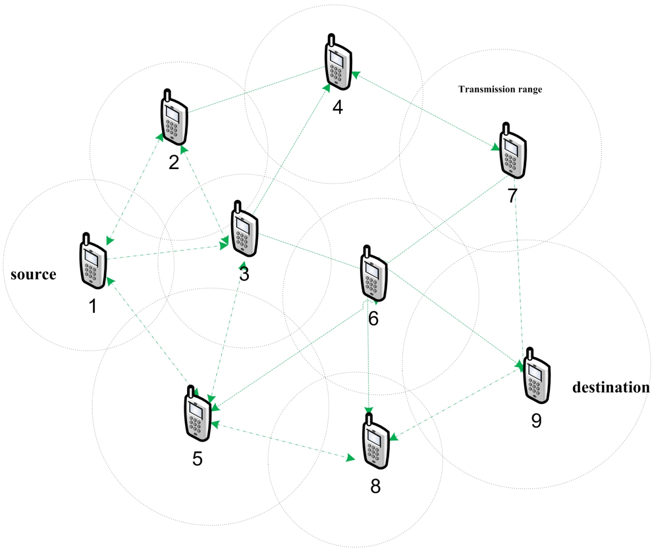

Figure 1. A MANET with nine cooperative nodes.

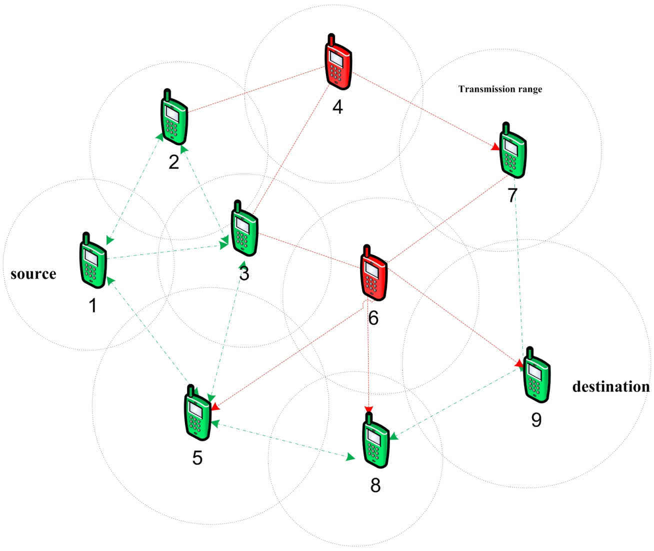

Figure 2. A MANET with two uncooperative nodes.

Consequently, if Node 2 or Node 3 wants to send a packet to Node 7, Node 8 or Node 9, it must go through Node 5. As a result of the totally selfish behaviours exhibited by Node 4 and Node 6, Node 5 is at a high risk of exhausting its limited energy resources due to the energy-constrained nature of nodes in MANETs. This type of behaviour creates an unfair environment if left unchecked. If Node 4 and Node 6 were cooperative, this will lessen the burden on Node 5, due to the fact that the amount of energy consumed during packet forwarding will be shared amongst the three nodes (with the assumption that the costs of the links of the three paths are almost the same). This will, in turn, elongate the life-time of the overall network.

3.2. Selective Dropping (Deceitful Behaviour)

A misbehaving node can act deceitfully in order to conserve its energy. It periodically participates in route discovery processes by forwarding control packets for other nodes. This is because control packets are smaller in size than data packets and consume a low amount of energy during transmission. Whenever a data packet is presented to this node for onward transmission, the data packet is dropped. Nodes that forward data packets to this node perceive the link as broken when they do not receive acknowledgements for the first set of data sent. The connection to this node is then deleted from their route entries, but after a given period, the connection is later re-added when the deceitful node participates in the route discovery process again.

4. The Proposed Reputation Management System

The proposed reputation model consists of a monitor, a reputation manager, a punishment scheme and a path administrator. The following assumptions are employed in our reputation management system.

i. Nodes in our network do not maliciously modify packets before forwarding.
ii. Every node operates in a promiscuous mode, such that each node listens to every packet transmitted by its neighbours, even if the packet is not intended for the node.
iii. A node may be selfish in terms of conservation of power and computing resources, but not malicious, which means that it will not try something that could directly target another node.

These assumptions are very important for the proposed model, because we are more focused on detecting nodes that exhibit totally selfish and deceitful behaviours in the network. A depiction of the various core components of the proposed model is given in Figure 3. These core components make up the modules of the reputation management system.

4.1. Monitoring Module (Monitor)

The monitor is an important part of the proposed model. It promiscuously listens to traffic and captures packets transmitted by a node. The monitor registers and records the number of packets being transmitted by a target node.

The monitor carries out a basic analysis for every captured packet to determine the type of packet being transmitted. It also checks if the node being observed (target node) is the originator of the packet or just a forwarder by comparing the source IP address of the packet against the IP address of the node being monitored. It has an inbuilt counter that increments and registers these data that are then stored in a node table.

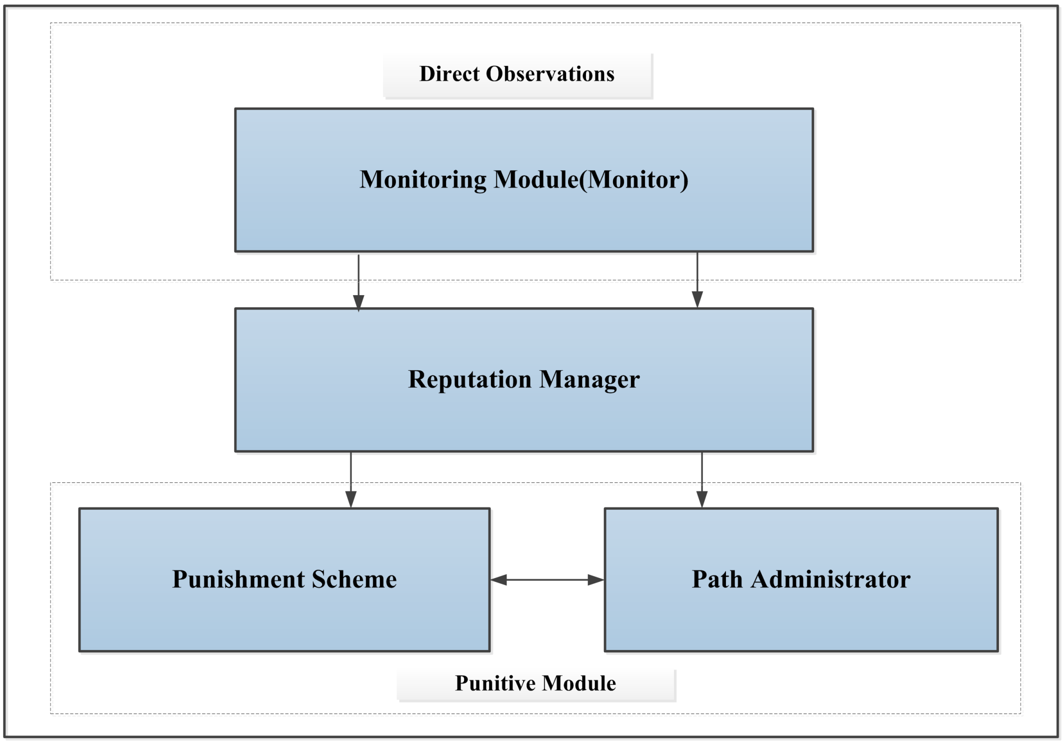

Figure 3. The schematic diagram of the reputation management system.

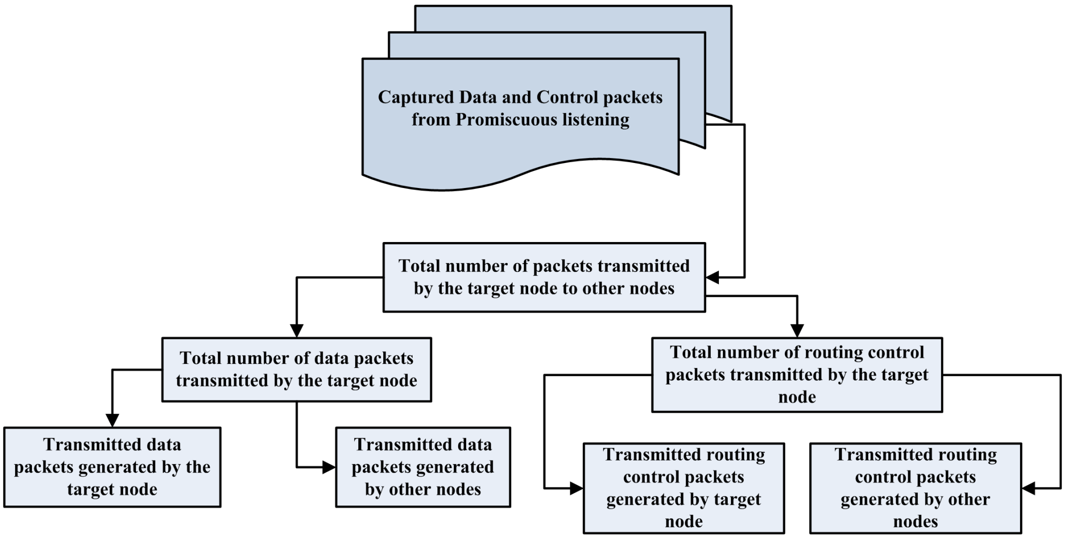
Captured Data and Control packets from Promiscuous listening
Total number of packets transmitted by the target node to other nodes
Total number of data packets transmitted by the target node
Total number of routing control packets transmitted by the target node
Transmitted data packets generated by the target node
Transmitted data packets generated by other nodes
Transmitted routing control packets generated by target node
Transmitted routing control packets generated by other nodes

Figure 4. Packet capturing and filtering in promiscuous mode.

Figure 4 gives insight into how the monitor captures and filters various packets using promiscuous listening. In order to cater to situations where a node has not had enough time to promiscuously listen to the traffic of its neighbours, the monitor relies on the packets that a node receives from its neighbours. Figure 5 shows how the received packets from the monitored node are filtered.

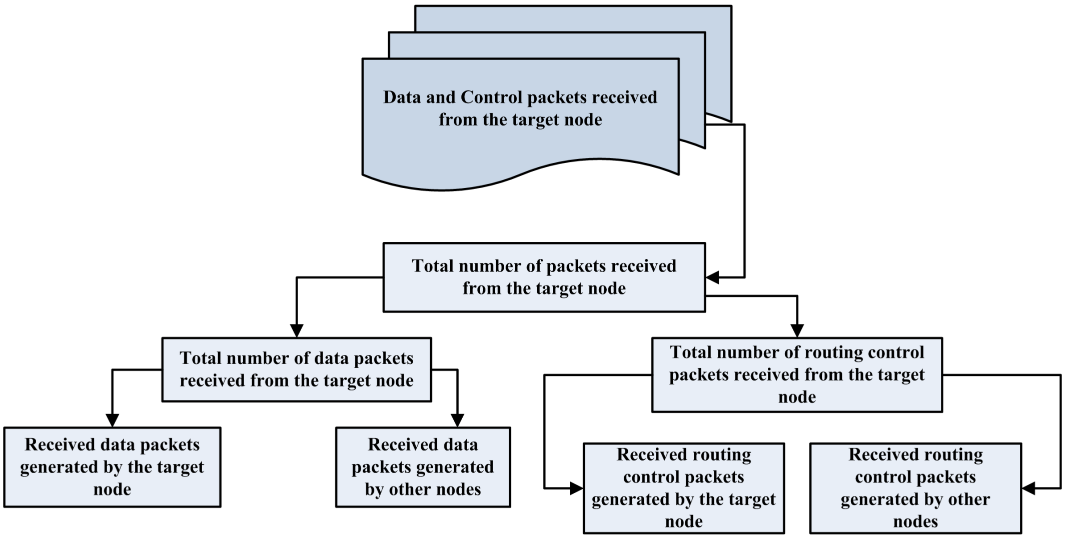
Data and Control packets received from the target node
Total number of packets received from the target node
Total number of data packets received from the target node
Total number of routing control packets received from the target node
Received data packets generated by the target node
Received data packets generated by other nodes
Received routing control packets generated by the target node
Received routing control packets generated by other nodes

Figure 5. Filtering of received packets.

For every packet it receives, the node analyses the packet to check if the sender is the originator or just a forwarder. Table 1 shows a brief summary of the information that could be derived from monitoring nodes' activities. The stored data are passed on to the reputation manager for onward computation.

Table 1. Summary of monitoring details stored in the node table.

Packet Variable	Packet Count Details
P_T	Packets transmitted by the target node.
P_{Tdata}	Data packets transmitted by the target node.
$P_{Tdata-self}$	Transmitted data packets generated by the target node.
$P_{Tdata-others}$	Transmitted data packets generated by other nodes.
$P_{Tcontrol}$	Routing control packets transmitted by the target node.
$P_{Tctrl-self}$	Transmitted routing control packets generated by the target node.
$P_{Tctrl-others}$	Transmitted routing control packets generated by other nodes.
P_{Rdata}	Data packets received from the target node.
$P_{Rdata-self}$	Data packets received from the target node generated by itself.
$P_{Rdata-others}$	Data packets received from the target node generated by other nodes.
$P_{Rcontrol}$	Control packets received from the target node.
$P_{Rctrl-self}$	Received routing control packets generated by the target node.
$P_{Rctrl-others}$	Received routing control packets from the target node generated by other nodes.

4.2. Reputation Manager

The reputation manager computes the reputation values of a node from the information it obtains from the monitor. Nodes generally consume more energy when they transmit data packets than routing control packets. The proposed reputation model focuses more on the number of data packets a node transmits for other nodes than the number of routing control packets it transmits. To compute the reputation of a node, we evaluate the information derived from the monitor in two phases.

Let $\hbar_{\mathbf{1}}$ represent the reputation of the node based on the data packets it transmits for others, and let $\psi_{\mathbf{1}}$ represent the reputation of the node based on the routing control packets it transmits for other nodes. We computed $\hbar_{\mathbf{1}}$ as shown in Equation (1):

$$\hbar_{\mathbf{1}}{=}P_{Tdata-others}/(P_{Tdata-self}+P_{Tdata-others}) \tag{1}$$

Similarly, $\psi_{\mathbf{1}}$ is given as:

$$\psi_{\mathbf{1}}{=}P_{Tctrl-others}/(P_{Tctrl-self}+P_{Tctrl-others}) \tag{2}$$

To compute the reputation of a node based on the number of data and routing control packets it receives from the target node, which was generated by other nodes, let $\hbar_{\mathbf{2}}$ represent the reputation value based on received data packets generated by other nodes and let $\psi_{\mathbf{2}}$ represent the reputation value based on received routing control packets generated by other nodes. We compute $\hbar_{\mathbf{2}}$ and $\psi_{\mathbf{2}}$ as follows:

$$\hbar_{\mathbf{2}}{=}\quad P_{Rdata-others}/(P_{Rdata-self}+P_{Rdata-others}) \tag{3}$$

$$\psi_{\mathbf{2}}{=}\quad P_{Rctrl-others}/(P_{Rctrl-others}+P_{Rctrl-self}) \tag{4}$$

The variables employed in computing the reputations $\hbar_{\mathbf{1}}$, $\psi_{\mathbf{1}}$, $\hbar_{\mathbf{2}}$ and $\psi_{\mathbf{2}}$ in Equations (1)–(4) are presented in Table 2.

Table 2. Terminology used in our proposed model.

Notation	Definitions
$\hbar_{\mathbf{1}}, \hbar_{\mathbf{2}}$	Reputations in terms of data packets transmitted.
$\psi_{\mathbf{1}}, \psi_{\mathbf{2}}$	Reputations in terms of routing control packets transmitted.
$\hbar_{\mathbf{data}}$	Final reputations in terms of data packets transmitted.
$\psi_{\mathbf{control}}$	Final reputations in terms of routing control packets transmitted.
$\mathfrak{h}_{\mathrm{T}}$	Evaluated total reputation.
$\mathfrak{h}_{0}$	Initial total reputation.
λ	Weight assigned to final reputations in terms of data packets transmitted.
ρ	Weight assigned to final reputations in terms of control packets transmitted.
ω	Decay factor for computed reputation value.

To compute the final reputation of a node in terms of data packets it has transmitted for other nodes, we combine $\hbar_1$ and $\hbar_2$. Thus, the final reputation of a monitored node in terms of data packets it has transmitted for other nodes is given as:

$$\hbar_{\mathbf{data}} = \quad \hbar_1 + \quad \hbar_{\mathbf{2}} \tag{5}$$

Similarly, the final reputation of the nodes based on the number of routing control packets it has transmitted for other nodes is given by:

$$\psi_{\mathbf{control}}{=}\quad \psi_{\mathbf{1}} + \quad \psi_{\mathbf{2}} \tag{6}$$

4.2.1. Total Reputation Value of Nodes

The total reputation of a node in the proposed model denoted by ɧ_{T} is the combination of the individual final reputation values of a node in terms of the data packets transmitted, $\hbar_{\mathbf{data}}$, and the routing control packets transmitted, $\psi_{\mathbf{control}}$. Mathematically, $\mathrm{R_T}$ is given by the equation below:

$$\text{ɧ}_{\mathbf{T}} = \quad \lambda\hbar_{\mathbf{data}} + \quad \rho\psi_{\mathbf{control}} \tag{7}$$

where λ and ρ are given as 0.8 and 0.2, respectively. The values of λ and ρ are based on the relative importance placed on the final reputation value of a node in regards to the type of packets it transmits continuously for other nodes.

4.2.2. Initial Reputation of Nodes in the Networks

At the onset of network operations, nodes in the network will not have interacted or have had the opportunity to monitor their neighbouring nodes for long enough time before computing their respective reputation values. In order to cater to this kind of situation, a default reputation value is introduced for all of the nodes in the network. This value is also assigned to a node that newly joins the network. From Subsection 4.2.1, we estimated that the total reputation of a node $\text{ɧ}_{\mathbf{T}}$ will always be between [0, 2]. Considering this range of values, the default reputation value for all nodes in the network is defined as $\text{ɧ}_{\mathbf{0}}$. This means that every node in the network is assigned a default reputation value, which is also their total reputation value at time t equal to zero. Mathematically, the total direct reputation of a node when they newly join the network or at the onset of network activities is given as:

$$\text{ɧ}_{\mathbf{T}} \quad = \quad \text{ɧ}_{\mathbf{0}} \tag{8}$$

After monitoring the various activities of nodes for a given period of time, a node would have gathered enough evidence to compute the individual reputation of its neighbouring nodes. The total reputation in this case is a combination of the initial default reputation value and the currently measured reputation value. Let us denote the new total reputation $\text{ɧ}_{\mathbf{T}}$ = $\text{ɧ}_{\mathbf{1}}$. We can evaluate the new total reputation $\text{ɧ}_{\mathbf{1}}$ as:

$$\text{ɧ}_{\mathbf{1}} = \quad \omega\text{ɧ}_{\mathbf{0}} + (1-\omega)\text{ɧ}_{\mathbf{M1}} \tag{9}$$

where ω is a small value between [0, 1] and $\mathbf{R_{M1}}$ is the currently measured reputation value of a node based on new evidence collected from monitoring activities. As more evidence becomes available, the direct reputation of the nodes will be regularly updated at a specific time interval. For instance, we evaluated the direct reputation of node at a given period of time t as $\text{ɧ}_{\mathbf{1}}$. We can therefore say that after a time interval of (t + 1), $\text{ɧ}_{\mathbf{2}}$ will be given as:

$$\text{ɧ}_{\mathbf{2}} = \quad \omega\text{ɧ}_{\mathbf{1}} + (1-\omega)\text{ɧ}_{\mathbf{M2}} \tag{10}$$

We can conclude that the direct total reputation of a node in our model can be evaluated using the equation below:

$$\text{ɧ}_{\mathbf{n}} = \quad \omega^{n}\text{ɧ}_{\mathbf{0}} + \omega^{n-1}(1-\omega)\text{ɧ}_{\mathbf{M1}} + \omega^{n-2}(1-\omega)\text{ɧ}_{\mathbf{M2}} + \omega^{n-i}(1-\omega)\text{ɧ}_{\mathbf{Mi}} \tag{11}$$

where $\text{ɧ}_{\mathbf{1}}$, $\text{ɧ}_{\mathbf{M2}}$ and $\text{ɧ}_{\mathbf{Mi}}$ are the newly-measured direct reputation values at regular intervals. Equation (11) can be further simplified as:

$$\text{ɧ}_{\mathbf{n}} = \quad \omega^{n}\text{ɧ}_{\mathbf{0}} + \sum_{i=1}^{n} \omega^{n-i}(1-\omega)\text{ɧ}_{\mathbf{Mi}} \tag{12}$$

where n = 1, 2, 3, . . . , i.

4.3. Punitive Module

The punitive module comprises the punishment scheme and the path administrator. These two modules ensure that nodes with total reputation values lower than the set threshold are dealt with as required.

4.3.1. Punishment Scheme

After evaluating the total reputation value of monitored nodes in our network, the values are stored in a node table and updated at regular intervals. After a period of time, it is expected that the total reputation value of a monitored node should increase if the node is transmitting data and routing control packets for other nodes. We defined a threshold value of 0.75, which is just a 25% increase in the initial default reputation value (0.6) assigned to all nodes at the onset of the network operations. The statuses of all monitored nodes are checked at regular intervals. The computed total reputation value of a node is mapped with a grading criterion, which helps to determine the status of a node.

Table 3 gives an overview of how the grading of the computed total reputation values is carried out by the nodes. When the status of a node is checked based on the computed total direct reputation value after a defined time interval, for example every 60 s, if the node status is flagged as "undecided", the node-ID of that node is placed on a watch-list within the punishment scheme. If subsequent node status checks still flag the node's status as "undecided", such that after two subsequent checks, the node status is changed to "bad node", the node is moved into a black-list within the punishment scheme. A node that is blacklisted will be denied network resources; all route requests that originate from it will be ignored. The node details are then passed on to the path coordinator, which checks the route cache and ensures that paths that contain that node are deleted, and an alternative route will be sourced for when needed. On the other hand, if a node is flagged as a "good node" or a "very good node", the node-ID is moved to a "white-list". Every node on the white-list is allowed to carry on with its normal network activities. Finally, when a node is flagged once as a bad node, the node is immediately blacklisted and its details passed to the path coordinator for immediate action.

Table 3. Grading criteria for the computed total reputation values.

Computed Reputation Value (R)	Grading Criteria	Node Status
1.000–2.000	Very good reputation	Very reliable node
0.750–0.999	Good reputation	Reliable node
0.500–0.749	Initial/normal/expected reputation	Undecided
0.000–0.499	Poor reputation	Unreliable node/bad node

4.3.2. Path Administrator

As already mentioned in Section 4.3, the path administrator ensures that nodes that are flagged as bad nodes are removed from the route cache. Its actions are based on the information it receives from the punishment scheme. The path administrator is integrated into the routing protocol, such that whenever a path is being sourced for sending a packet, it checks to ensure that the packet will not be sent via a path that contains a node that has been black-listed.

5. Implementation and Simulations

We designed and programmed the modules described above using C++ and implemented the various classes to work with existing NS-2.34 modules [45]. Several modifications were also carried out on existing NS-2.34 modules to incorporate the various required node behaviours and the overall functionality of the proposed reputation management model. Dynamic source routing was used as the routing protocol to verify the functionalities of the proposed model. Exhaustive simulations were also carried out, averaging 10 simulations for each specified scenario. Other general parameters used are mentioned in Table 4.

Table 4. Parameters of the simulations. CBR, constant bitrate.

Parameters	Values
Topographical area	900 m × 900 m
Simulation time	900 s
Channel type	WirelessChannel
Radio-propagation mode	TwoRayGround
Antenna type	Antenna/OmniAntenna
Interface queue type	CMUPriQueue
Maximum packet in queue	50
Network interface type	Phy/WirelessPhy
Link layer type	LL
MAC type	802.11
Number of connections	12
Traffic type	CBR
Data packet size	512 bytes
Number of mobile nodes	20
λ,ρ,ω	0.8, 0.2, 0.1
Behaviour Types	Good, selfish, deceitful nodes

5.1. The Implemented Behaviours

The simulated nodes were programmed to exhibit three different behaviours during the course of the simulations. The behaviours exhibited by these nodes are briefly described below:

i. Good nodes: A good node in our model responds to all route requests and ensures that all of the data and routing control packets that are meant for other nodes are forwarded to the next hop node or the recipient node if they are the last hop in the path.

ii. Selfish nodes: These nodes do not respond to any route requests received from other nodes, this ensures that they do not forward data and routing control packets for other nodes. Their existence is only known to other nodes when they need to send their own packets.

iii. Deceitful nodes: Deceitful nodes sporadically reply to the route requests from other nodes, but ensure that all of the data packets that are meant for forwarding are dropped. For instance, a deceitful node drops one out of every three routing control packets that it receives and ensures that every data packet it receives for forwarding is dropped.

5.2. Network Performance Evaluation

For the purpose of evaluation, we use the following network metrics in our study:

i. Packet delivery ratio: This is the ratio between the amount of data packets received and the amount of data packets sent. The packet delivery ratio can also be interpreted as the ratio of the number of packets received at the constant bitrate (CBR) sink to the number of packet sent by the CBR source.

ii. Routing overhead: This is defined as the total number of routing control packets transmitted.

iii. Throughput: Network throughput refers to the average data rate of successful data or message delivery over a specific communications link.

iv. End to end delay: The end to end delay of a packet is defined as the time a packet takes to travel from the source to the destination.

6. Results and Analysis

This section presents the simulation results that show the effects of an increase in the presence of selfish and deceitful nodes in networks. Furthermore, it also analyses how the deployment of the proposed reputation model is able to curb and mitigate the negative effects of the increased presence of these nodes in the network.

6.1. Packet Delivery Ratio

Figures 6 and 7, present the packet delivery ratio for the networks experiencing a gradual increase in the number of selfish and deceitful nodes with and without the deployed reputation model. When the performance of the networks shown in Figure 6 is analysed, a gradual increase in the number of selfish nodes operating in the networks led to a decrease in the packet delivery ratio of the networks. As observed in Figure 6, selfish nodes do not participate in route discovery processes, which exempts them from being presented packets for forwarding to other nodes in the network. Hence, there will be a high demand on the good nodes to forward packets for other nodes, such that the good nodes will be heavily relied on to deliver more and more data packets to the required destinations. This constitutes a huge task for the services these good nodes can offer to other nodes in the network. Thus, there is a possibility that some packets may be lost, and packet collision may also increase, which could also lead to further decline in the packet delivery ratio. The slightly improved packet delivery ratio recorded by the deployed reputation model is a result of the punishment module, which eliminates and isolates the detected selfish nodes and ensures that only reliable nodes (good nodes) use the network resources to transmit packets, which are delivered to the required destinations.

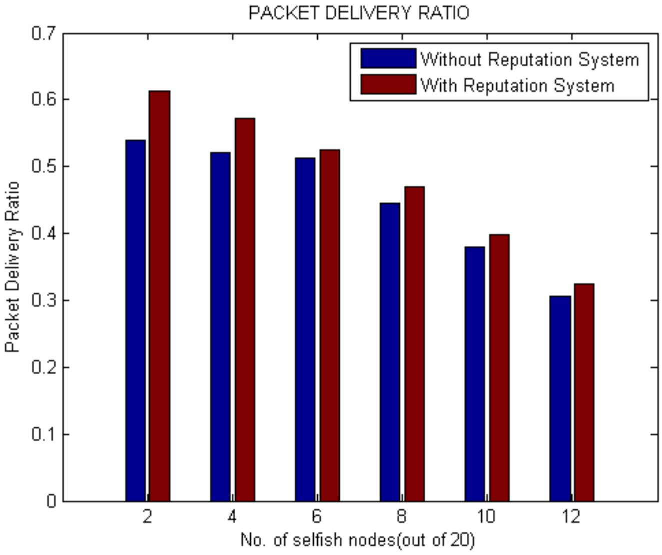

Figure 6. Packet delivery ratio for networks experiencing an increase in selfish nodes.

Similarly, from Figure 7, it is observed that as the number of deceitful nodes continues to increase in the network (2, 4, 6, 8, . . . , 12), the packet delivery ratio of the network gradually decreases. This is expected as a result of the smaller number of good nodes forwarding data packets and more data packets being dropped by these deceitful nodes.

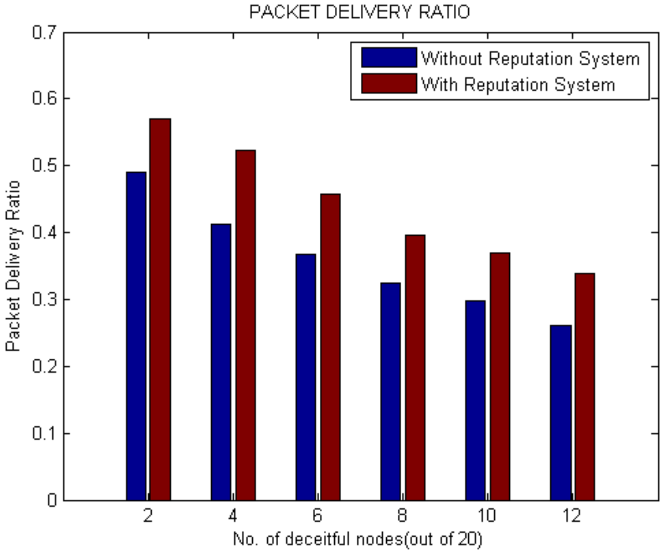

Figure 7. Packet delivery ratio for networks experiencing an increase in selfish nodes.

It is also observed from Figure 7 that the deployment of the reputation model improved the packet delivery ratio of the network. For all of the cases whereby a decline in the packet delivery ratio occurred as a result of more deceitful nodes, the networks with the reputation model registered a much improved packet delivery ratio, which is from 15%–20% in some cases. This improved packet delivery ratio recorded by the reputation model is mostly a result of more data packets being delivered due to the isolation and prevention of these deceitful nodes accessing the limited resources. Furthermore, the improved packet delivery ratio may also be a result of reduced packet collision in the network due to a few good nodes contending for limited bandwidth.

6.2. Routing Overhead

As shown in Figure 8, a downward trend could be observed as regards the amount of routing control packets in circulation in both networks as the number of selfish nodes in the networks increases. This is most likely due to fewer good nodes participating in the route discovery and route management processes for other nodes. As mentioned earlier, these selfish nodes do not participate in the route discovery processes for other nodes in the network. The number of routing control packets circulating in the network when the proposed reputation model was deployed is less compared to the network without the reputation model. This is expected, because when the selfish nodes are detected in the reputation model, they are deleted from the routing path and are denied network access, such that route requests from these nodes are ignored. This means that fewer route requests, route replies and route error packets will always be in circulation due to the isolation.

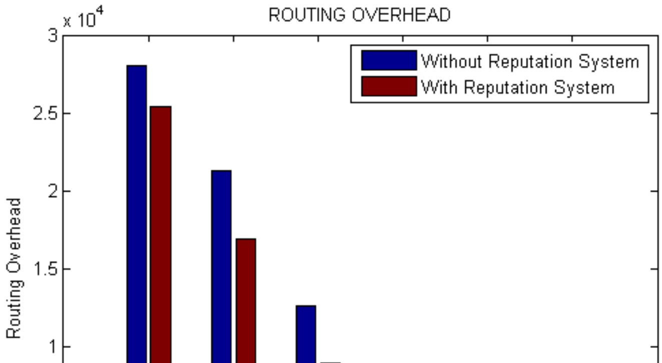

Figure 8. Routing overhead for networks experiencing an increase in selfish nodes.

Similarly, it is observed in Figure 9 that there is also a gradual decrease in the number of routing control packets circulating in the networks as the number of selfish nodes increased from two to 12 gradually. One significant difference between Figures 8 and 9 is in the amount of routing control packets in circulation as the number of selfish and deceitful nodes increases in the networks with and without the reputation model, respectively. This difference is due to the un-identical behaviour patterns, such that selfish nodes do not participate in route discovery or the route management process for other nodes. On the other hand, the deceitful nodes periodically participate in route discovery and management processes for other nodes. Hence, for the network with deceitful nodes, more routing control packets are in circulation compared to the network with selfish nodes.

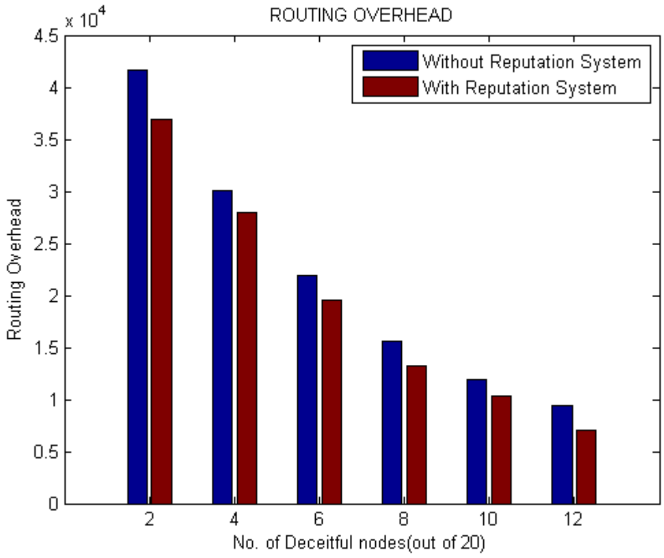

Figure 9. Routing overhead for networks experiencing an increase in deceitful nodes.

6.3. Throughput

As observed in Figure 10, an increase in the number of selfish nodes in the network results in a gradual decrease in the network throughput. This is a result of fewer data packets being delivered to the desired destination. When comparing the networks without the reputation model to the networks with the reputation model, the same trend of a reduction in the network throughputs is observed. However, the networks with the reputation model have a better network throughput performance. The improved network throughputs could be a result of fewer nodes utilizing the available bandwidth after the selfish nodes are blacklisted.

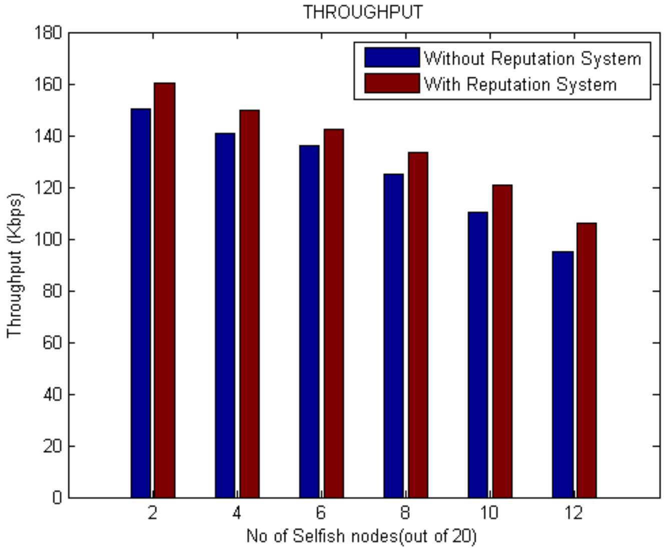

Figure 10. Throughput for networks experiencing an increase in selfish nodes.

The reputation model also increases the proportion of packets that reach the final destination by re-routing the packets to avoid blacklisted nodes. Additionally, since selfish nodes are blacklisted when detected through the computed reputation values, the act of ignoring their route requests means that they are not able to send their own data packets. Thus, a possible reduction in packet collision may most likely improve the network throughput.

Similarly, when the throughput of the networks with the reputation model and the networks without the reputation model are compared in the presence of an increased number of deceitful nodes, as observed in Figure 11, as the number of the deceitful nodes increases, the network throughputs decrease due to many fewer data packets being delivered to their respective destinations. Similarly, the improved network throughput observed in the network with the reputation model may also be a result of the ability of the network to isolate the deceitful nodes. The reputation model ensures that only nodes in the white-list and watch-list participate in network activities and results in reduced packet collision. It is also observed that the deceitful nodes reduce that network throughput more than the selfish nodes due to the behaviours, *i.e.*, continuously dropping data packets presented for forwarding.

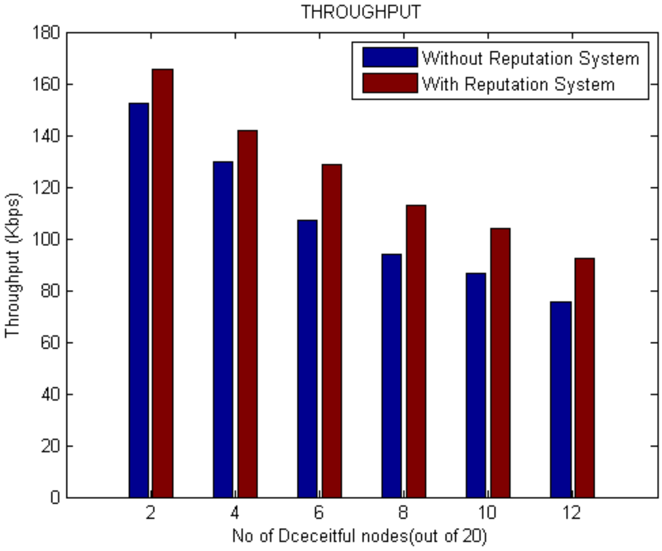

Figure 11. Throughput for networks experiencing an increase in deceitful nodes.

6.4. End to End Delay

In the networks without the reputation model, as shown in Figure 12, as the presence of selfish nodes gradually increased from 2 → 8, the network end to end delay decreased gradually. A slight increase in the delay was also observed when the number of selfish nodes increased from 8 → 12. The decrease in the end to end delay is due to fewer good nodes participating in packet routing activities. Since the selfish nodes do not participate in route discovery processes, their increased presence may partition the network, which, in turn, reduces the amount of time it takes to send and receive packets between the good nodes that remain in the various partitions. Increased presence of selfish nodes also means that there is a possibility of experiencing reduced packet collisions in the network. Their non-participation in route discovery processes may ensure that data transfer between established genuine links (between two good nodes) may be quicker due to fewer packets competing for bandwidth.

On the other hand, the slight increase in the delay experienced by the networks when the number of selfish nodes increase from 8 → 12 could be a result of different factors. As observed in Figure 12, the registered increase in the delay is minimal and could be a result of increased hop counts from the source to the destination when data are being transferred between good nodes in disjoint partitions.

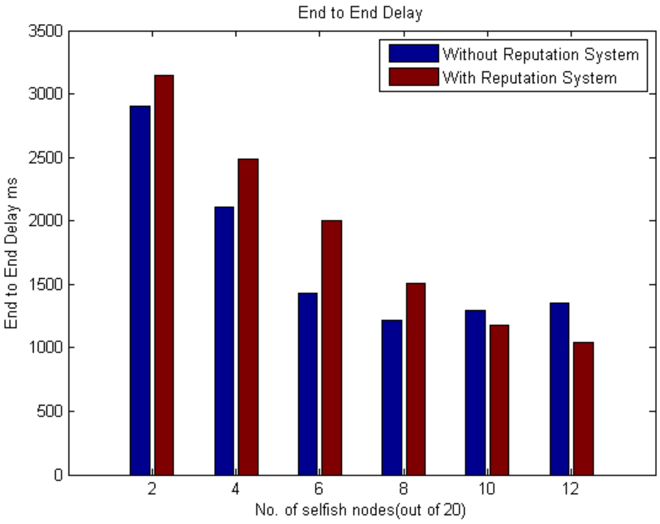

Figure 12. Overall end to end delay for networks experiencing an increase in selfish nodes.

When compared to the networks with the deployed reputation model, the end to end delays are higher than the networks without the reputation model as the number of selfish nodes increased from 2 → 8. As the number of selfish nodes increases from 10 → 12, the end to end delays of the network slightly decrease when compared to the network without the reputation model. The higher end to end delay in the reputation model may be a result of the additional time it takes to check if a node is on the white-list, watch-list or blacklist before responding to the route request from that node. It may also be a result of the activities of the path coordinator to source paths without bad nodes before routing a packet.

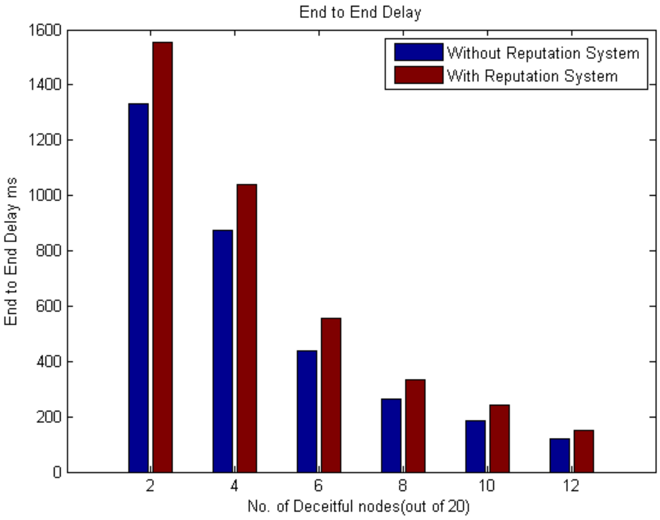

Figure 13. End to end delay for networks experiencing an increase in deceitful nodes.

When comparing the performance of the networks in Figures 12 and 13, a trend toward a decrease in the network delays as both sets of misbehaving nodes increase is observed. The networks with deceitful nodes had a much lower end to end delay when compared to the networks with selfish nodes. Deceitful nodes periodically respond to route requests and drop the corresponding data packets. This may lead to decreased end to end delays due to less queuing at the interface queue and buffering during route discovery latency.

6.5. Discussion

Simulation results show that the deployed reputation model is effective at detecting and isolating misbehaving nodes. The analysis of the results of the simulated networks shows that the network with the reputation model experiences a slightly higher end to end delay than the networks without the model. However, the network with the reputation model has a much better performance in terms of the throughputs, packet delivery ratios and lower routing overheads. This suggests that the deployed reputation model is beneficial to MANETs.

The registered network end to end delays with the deployed reputation model means that packets may take longer to get to their desired destination, which demonstrates that to accomplish a reliable MANET using the deployed reputation model, the possible increase in the average end to end of a network serves as the compromise. However, the trade-off between average end to end network delays and the other network metrics, that is better network throughput, packet delivery ratio and lower routing overhead, confirms that deployment of the proposed reputation model could lead to an improvement of the overall performance of a MANET.

The effectiveness of the proposed dynamic reputation management system could be further established by comparing the improved network metrics recorded with the deployed reputation model with another proposed reputation model. However, the main motivation for the monitoring and detection technique proposed in this paper is to monitor, detect and curb the negative effects of selective existence attacks carried out by selfish nodes that do not participate in route discovery processes for other nodes in a MANET, as described in Subsection 3.1. This attack has not been addressed by most existing reputation managements systems.

7. Conclusions

The proposed dynamic reputation management system describes a novel technique of observing the packet transmission activities of mobile nodes in the network. Although existing monitoring techniques have been successful in observing several misbehaviours of nodes in MANETs, selective existence attacks carried out by a special type of selfish node will go undetected with the deployment of the existing monitoring schemes. This paper further describes a unique way of observing and analysing the packet transmission activities of such behaviours and other selfish behaviours. The proposed reputation model is capable of mitigating the adverse effects in the presence of these types of misbehaving nodes (selfish and deceitful behaviours) on the scarce network resources. The presence of these misbehaving nodes in a mobile network is detrimental to good nodes. These good nodes consume their limited energy by participating in all network activities as required in a MANET. Future research work will focus on how to compensate the good nodes for consuming their limited energy in forwarding packets for other nodes in the network.

Author Contributions

This paper was the result of collaboration among the three authors. The research theme and idea were proposed by Eric Chiejina and further refined by Hannan Xiao. Eric Chiejina and Hannan Xiao were mainly involved in developing the reputation model. Extensive simulations for testing and verifying the developed reputation model were carried out by Eric Chiejina. The result analyses were carried out by Bruce Christianson, Hannan Xiao and Eric Chiejina. All authors contributed to the writing of the paper, the literature review and the discussion of the obtained results. The three authors have read and approved the final version of the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Giordano, S. Mobile ad hoc networks. In *Handbook of Wireless Networks and Mobile Computing*; Wiley: River Street Hoboken, NJ, USA, 2002; pp. 325–346.
2. Papadimitratos, P.; Haas, Z.J. Secure Routing for Mobile Ad Hoc Networks. In Proceedings of the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, USA, 27–31 January 2002; pp. 193–204.
3. Senthilkumar, S.; William, J. A Survey on Reputation Based Selfish Node Detection Techniques In Mobile Ad Hoc Network. *J. Theor. Appl. Inf. Technol.* **2014**, *60*, 208–215.
4. Cho, J.H.; Swami, A.; Chen, I.R. *Mission-Dependent Trust Management in Heterogeneous Military Mobile Ad Hoc Networks*; Technical Report, DTIC Document; Defense Technical Information Center: Fort Belvoir, VA, USA, 2010.
5. Velloso, P.B.; Laufer, R.P.; de O. Cunha, D.; Duarte, O.C.M.B.; Pujolle, G. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Trans. Netw. Serv. Manag.* **2010**, *7*, 172–185.
6. McQuillan, J.M.; Richer, I.; Rosen, E. The new routing algorithm for the ARPANET. *IEEE Trans. Commun.* **1980**, *28*, 711–719.
7. Marti, S.; Giuli, T.J.; Lai, K.; Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000; pp. 255–265.
8. Banerjee, A.; Neogy, S.; Chowdhury, C. Reputation based trust management system for MANET. In Proceedings of the 2012 Third International Conference on Emerging Applications of Information Technology (EAIT), West Bengal, India, 30 November–1 December 2012; pp. 376–381.
9. Sun, Y.L.; Han, Z.; Yu, W.; Liu, K.R. Attacks on trust evaluation in distributed networks. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006; pp. 1461–1466.
10. Liu, J.; Fu, F.; Xiao, J.; Lu, Y. Secure routing for mobile ad hoc networks. In Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence,

Networking, and Parallel/Distributed Computing, 2007 (SNPD 2007), 30 July–1 August 2007; Volume 3, pp. 314–318.

11. Denko, M.K. Detection and prevention of Denial of Service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme. *J. Syst. Cybern. Inform.* **2005**, *3*, 1–9.
12. Yan, Z.; Zhang, P.; Virtanen, T. Trust evaluation based security solution in ad hoc networks. In Proceedings of the Seventh Nordic Workshop on Secure IT Systems, Gjøvik, Norway, 15–17 October 2003; Volume 14.
13. Theodorakopoulos, G.; Baras, J.S. Malicious users in unstructured networks. In Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), Anchorage, AK, USA, 6–12 May 2007; pp. 884–891.
14. Shabut, A.M.; Dahal, K.; Awan, I. Enhancing Dynamic Recommender Selection Using Multiple Rules for Trust and Reputation Models in MANETs. In Proceedings of the 2013 IEEE 25th International Conference on Tools with Artificial Intelligence (ICTAI), Herndon, VA, USA, 4–6 November 2013; pp. 654–660.
15. Ayday, E.; Fekri, F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks. *IEEE Trans. Mob. Comput.* **2012**, *11*, 1514–1531.
16. Ayday, E.; Lee, H.; Fekri, F. Trust management and adversary detection for delay tolerant networks. In Proceedings of the IEEE Military Communications Conference (2010-MILCOM), San Jose, CA, USA, 31 October–3 November 2010; pp. 1788–1793.
17. Ayday, E.; Fekri, F. BP-P2P: Belief propagation-based trust and reputation management for P2P networks. In Proceedings of the 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Seoul, Korea, 18–21 June 2012; pp. 578–586.
18. Buttyán, L.; Hubaux, J.P. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of the 1st ACM International Symposium on Mobile Ad Hoc Networking & Computing, Boston, MA, USA, 2000; IEEE Press: Hoboken, NJ, USA, 2000; pp. 87–96.
19. Buttyán, L.; Hubaux, J.P. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mob. Netw. Appl.* **2003**, *8*, 579–592.
20. Jakobsson, M.; Hubaux, J.P.; Buttyán, L. A micro-payment scheme encouraging collaboration in multi-hop cellular networks. In *Financial Cryptography*; Springer: Berlin, Germany, 2003; pp. 15–33.
21. Zhong, S.; Chen, J.; Yang, Y.R. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proceedings of the IEEE Societies Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003), San Francisco, CA, USA, 30 March–3 April 2003; Volume 3, pp. 1987–1997.
22. Félegyházi, M.; Buttyán, L.; Hubaux, J.P. Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks–the static case. In *Personal Wireless Communications*; Springer: Berlin, Germany, 2003; pp. 776–789.
23. Cai, J.; Pooch, U. Allocate fair payoff for cooperation in wireless ad hoc networks using shapley value. In Proceedings of the 18th International Parallel and Distributed Processing Symposium, Santa Fe, NM, USA, 26–30 April 2004; p. 219.

24. Chiejina, E.; Xiao, H.; Christianson, B. A Candour-based Trust and Reputation Management System for Mobile Ad Hoc Networks. In Proceedings of the 6th York Doctoral Symposium on Computer Science & Electronics, York, UK, 29 October 2013; University of York: York, UK, 2013.
25. Michiardi, P.; Molva, R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Advanced Communications and Multimedia Security*; Springer: Berlin, Germany, 2002; pp. 107–121.
26. Buchegger, S.; Le Boudec, J.Y. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, 9–11 January 2002; pp. 403–410.
27. Bansal, S.; Baker, M. *Observation-Based Cooperation Enforcement in Ad Hoc Networks*; Cornell University: Ithaca, NY, USA, 2003.
28. Virendra, M.; Jadliwala, M.; Chandrasekaran, M.; Upadhyaya, S. Quantifying trust in mobile ad-hoc networks. In Proceedings of the IEEE International Conference of Integration of Knowledge Intensive Multi-Agent Systems (KIMAS), Waltham, MA, USA, 18–21 April 2005.
29. He, Q.; Wu, D.; Khosla, P. A secure incentive architecture for ad hoc networks. *Wirel. Commun. Mob. Comput.* **2006**, *6*, 333–346.
30. Li, J.; Li, R.; Kato, J. Future trust management framework for mobile ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 108–114.
31. Buchegger, S.; Le Boudec, J.Y. Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland, 9–11 June 2002; ACM: New York, NY, USA; pp. 226–236.
32. Hu, J.; Burmester, M. Cooperation in mobile ad hoc networks. In *Guide to Wireless Ad Hoc Networks*; Springer: Berlin, Germany, 2009; pp. 43–57.
33. Buchegger, S.; Le Boudec, J.Y. *A Robust Reputation System for Peer-to-Peer and Mobile Ad-Hoc Networks*; P2PEcon 2004, No. LCA-CONF-2004-009; Harvard University: Cambridge, MA, USA, 2004.
34. Zouridaki, C.; Mark, B.L.; Hejmo, M.; Thomas, R.K. A quantitative trust establishment framework for reliable data packet delivery in MANETs. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 7 November 2005; ACM: New York, NY, USA, 2005; pp. 1–10.
35. Zouridaki, C.; Mark, B.L.; Hejmo, M.; Thomas, R.K. Robust cooperative trust establishment for MANETs. In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 30 October–3 November 2006; ACM: New York, NY, USA; pp. 23–34.
36. Pirzada, A.A.; McDonald, C. Trust establishment in pure ad-hoc networks. *Wirel. Pers. Commun.* **2006**, *37*, 139–168.
37. Boukerche, A.; Ren, Y. A security management scheme using a novel computational reputation model for wireless and mobile ad hoc networks. In Proceedings of the 5th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Vancouver, BC, Canada, 27–28 October 2008; ACM: New York, NY, USA; pp. 88–95.

38. Li, N.; Das, S.K. A trust-based framework for data forwarding in opportunistic networks. *Ad Hoc Netw.* **2013**, *11*, 1497–1509.
39. Kumar, S.G.C. A Novel Routing Strategy for Ad Hoc Networks with Selfish Nodes. *J. Telecommun.* **2010**, *3*, 23–28.
40. Gong, W.; You, Z.; Chen, D.; Zhao, X.; Gu, M.; Lam, K.Y. Trust based routing for misbehavior detection in ad hoc networks. *J. Netw.* **2010**, *5*, 551–558.
41. Gong, W.; You, Z.; Chen, D.; Zhao, X.; Gu, M.; Lam, K.Y. Trust based malicious nodes detection in MANET. In Proceedings of the International Conference on IEEE E-Business and Information System Security, 2009 (EBISS'09), Wuhan, China, 23–24 May 2009; pp. 1–4.
42. Bakar, K.A.A.; Irvine, J. A Scheme for Detecting Selfish Nodes in MANETs using OMNET++. In Proceedings of the 2010 6th International Conference on Wireless and Mobile Communications (ICWMC), Valencia, Spain, 20–25 September 2010; pp. 410–414.
43. Tamilarasi, M.; Sundararajan, T. Secure Enhancement Scheme for Detecting Selfish Nodes in Manet. In Proceedings of the 2012 International Conference on Computing, Communication and Applications (ICCCA), Tamilnadu, India, 22–24 February 2012; pp. 1–5.
44. Vigna, G.; Gwalani, S.; Srinivasan, K.; Belding-Royer, E.M.; Kemmerer, R.A. An intrusion detection tool for AODV-based ad hoc wireless networks. In Proceedings of the 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, 6–10 December 2004; pp. 16–27.
45. Fall, K.; Varadhan, K. The ns Manual (2011). Available online: http://www. isi. edu/nsnam/ns/doc/ns doc. pdf (accessed on 16 April 2015).