Hybrid Watchdog and Pathrater algorithm for improved security in Mobile Ad Hoc Networks

N. Soganile¹, T. Baletlwa², and B. Moyo²
¹,³ Department of Computer Science and Information Systems, University of Venda, Thohoyandou, Limpopo, South Africa
² Department of Computer Science, Botho University, Gaborone, Botswana

Abstract—Mobile hosts have a new wireless networking paradigm, called ad hoc networks. These networks do not rely on fixed infrastructures, like traditional wireless networks. To sustain connectivity hosts rely on each other for all communication transactions. The unique properties of ad-hoc networks are promoting an increased trend towards their adoption. The military and other security sensitive operations were the main and first application areas of ad hoc networks, but the trend has shifted now, businesses are relying on them. Mitigating the vulnerability of these networks to security attacks remains the main design challenge for these types of networks. A serious problem common in mobile ad-hoc networks (MANets) is the black hole attacks. The challenge of detecting and eliminating blackhole attacks in mobile ad-hoc networks, has led to poor network performance. This paper focuses on vulnerabilities of MANets and in particular it looks at the blackhole attacks. We present the design of an improved Watchdog and Pathrater algorithm called Radical Watchdog and Pathrater Algorithm for detecting and eliminating Black hole attacks. We carry out an extensive literature review and also make an analysis of the existing techniques for detection and elimination of Blackhole attacks in MANets. Our work culminates with the design of a RWP algorithm for improved security in MANets.

Keywords: Mobile Networks, Black hole, MANets, Security technique, Intrusion detection,

1 Introduction

Technology is expanding every day, forcing a change in communication trends. Mobile Ad-hoc networks are a new paradigm of wireless communication, for mobile hosts. Unlike traditional networks, Mobile Ad-hoc networks do not rely on any fixed infrastructure, or any centralized control, such as base stations, or mobile switching centres. The mobile nodes communicate using a wireless network [1]. According to [2] the Mobile Ad-hoc network hosts are mobile and flexible, and they communicate with each other within radio range, through direct wireless links, or multi hop routing. Due to its mobility and portability in wireless communication, it introduces data security threats, and security attacks. Das [3] states that routing protocols in Mobile Ad-hoc networks are there to set up the most suitable path, between the source and destination, with minimum overhead, and minimum bandwidth consumption, so that packets are delivered in a timely manner. These suitable paths are known as “mini hops”. “Routing protocols are usually engaged to determine the routes, following a set of rules that enable two or more devices to communicate with each other” [4]. In MANets routes are enabled in between the mobile hosts, using multi hop, as the transmission range of wireless radio is limited. The mobile hosts are responsible for passing through packets over Mobile Ad-hoc networks, and they are not aware of the topology of the network. Routing plays an important role in the security of the entire network. The mobility and portability in Mobile Ad-hoc networks introduces security threats and security attacks. A change in topology means that security will have to be accessible, as nodes may be mobile, entering and leaving the network [5]. Mobile Ad-hoc networks are vulnerable to attacks that can be categorized into two types: Passive attacks and Active attacks, where active attacks can further be subdivided into internal and external attacks. Mobile Ad-hoc networks routing protocols are exposed to different types of attacks, Black-hole attacks, being the most serious type.

[6] states that “Black-hole attack is a specific type of attack, where a malicious node injects false route replies to the route requests it receives, by advertising itself as having the shortest path to a destination”. Therefore, the fake replies can be counterfeited to deflect network traffic through the malicious node, for eavesdropping, or simply to attack all traffic to it, in order to perform a Denial of Service (DoS) attack, by dropping the received packets. Although the performance of Mobile Ad-hoc networks under Black-hole attacks can be improved, by accurately detecting and eliminating Black-hole nodes, there are however indications which specifically suggest that the inaccurate detection and elimination of Black-hole attacks in Mobile Ad-hoc networks, can result in poor network performance [7].

1.1 Problem Statement

The increasingly developing trend of information and communication technology has not only provided our world with unequaled rewards, but has correspondingly created a conducive environment for manifold security challenges. Ad-
hoc networks for instance, though a new and innovative wireless networking paradigm, are yet cheap prey to malicious attacks, due to their portability and mobility. This security weakness places huge demand for effective and accurate techniques, for detecting and eliminating threats such as Black-hole attack, to guarantee satisfactory performance in MANets. The concern here is to analyse existing security techniques in MANets, and suggest an approach to more effectively detect, and eliminate black hole attacks.

2 Ad-hoc networks

Subir [8] states, “Ad-hoc networks are a collection of wireless mobile nodes, which form a network without the use of any fixed infrastructure, or centralized control such as a base station”. Mobile nodes are free to move randomly, and organize themselves, therefore the networks wireless topology may change rapidly and unpredictably. The birth of Ad-hoc networks is informed by the desire to improve upon the operational efficiency, and indeed performance of mobile networks. Eliminating the need for huge infrastructure, and centralized controls in Ad hoc networks is one of the brains behind their exploit [9]. These networks are classified into First generation (used for different military scenarios e.g. Packet radio networks), Second generation (used for the same purpose as the first generation ad-hoc networks system, but included further advancements, such as Global mobile information Systems, Near term Digital Radio (NTDR)), Third generation ad-hoc network systems, are also known as commercial ad-hoc network systems e.g. Bluetooth, ad-hoc sensor networks etc [10]. Such networks introduce redundant communication paths, which tend to improve fault tolerance for the network. Additionally, data packets are given the ability to "hop" from one user to another, thereby effectively extending the network coverage area; a solution to overcome non-line of sight (LOS) issues [9]. Computer devices and other devices operate in a peer-to-peer mode, in wireless topology without any access points, or centralized control such as base stations, as all devices communicate directly with other devices [11]. However, the deployment of mobile application required fast and widespread changes in topology, which possess a huge challenge to the mesh topology obtainable in ad hoc networks.

This gave rise to the different categories of ad hoc networks. Ad-hoc networks can be categorized into static and mobile ad hoc networks.

2.1 Mobile Ad-hoc Networks (MANets)

According to [12], Mobile Ad-hoc Networks have attracted most attention from many researchers world over. Deng [13] highlights that “Mobile Ad-hoc Networks are a collection of mobile nodes, which communicate with each other, and are connected to each other through wireless links”. These mobile nodes are not fixed to any centralized control, like base stations or mobile switching centres, and there is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. In the work by Kumar [14], all mobile agents or devices in MANets, are described as being “autonomous”.

As stated earlier, mobile ad hoc networks are innovative offshoots of the traditional ad hoc networks. The additional challenge of extreme network flexibility, placed upon ad hoc networks by mobile applications, requires a technology which ensures quick and accurate update of communication routes. Moreover, MANets have the capability to do so. “MANets are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility” [9]. MANets can be implemented as self-contained networks, or linked up to the internet, or private networks. The second style of setup is called hybrid MANets. In MANets, a network of self-configuring routers, connected via wireless links, is created forming a random topology. Furthermore, because such routers are highly mobile, and can quickly organize themselves at random, the topology of the wireless network changes rapidly and unpredictably. In a mobile ad hoc network there could be a great variety of mobile devices participating as autonomous nodes, either sending or receiving data from others within the network, as shown below.

Figure 1: Mobile Ad-hoc Network

2.2 Features of MANets

The mobile ad hoc network has a number of features enumerated by [12] to include the following:

- Constantly changing topology, due to the continuous motion of nodes
- Unreliability of wireless links between nodes
- Lack of incorporation of security features, in statically configured wireless routing protocol, not meant for ad hoc environments
- Absence of Centralized Management

The above features, according to [12], are the reason why Mobile Ad-hoc networks are more prone to suffer several security challenges, caused by the malicious behaviors of nodes, other than the traditional wired networks.
2.3 Challenges of MANets

The common challenges faced by MANets is summarized by the following list:

- Limited bandwidth:
- Dynamic topology
- Mobility-induced route changes
- Battery constraints
- Security threats

2.4 Vulnerabilities in MANets

Every network is vulnerable in one way or the other, to one form of attack or the other. In the case of MANets, their vulnerability to attacks is higher than on the wired networks. In [15], some of the major vulnerabilities are listed as Lack of Centralized Management, No Predefined Boundary, Cooperativeness, Limited Power Supply, and Adversary inside the Network. The last weakness bothering security, forms the core of our work. As part of the multiple security concerns in MANets, we consider Black-hole attacks on MANets.

2.5 Black-hole Attack

The mobile nodes within MANets can freely join, and leave the network at any time [16]. This flexibility also introduces a security challenge, where a malicious node can pretend to be a legitimate member of the network, for purpose of compromising the security of the nodes. It is hard to detect that the behaviour of the node is malicious. Thus, this attack is more dangerous than an external attack [16]. The Black-hole attack actually falls under the category of attacks known as Network Layer Attacks.

The basic idea behind this kind of attack is that the intruding node injects itself into the active path from source to destination, or to absorb network traffic[16]. Technically, in a black-hole attack, the malicious node claims to have an optimum route to the node, whenever it receives route request (RREQ) packets, and sends the response packet (REPP) with highest destination sequence number, and minimum hop count value, to the originator node, whose RREQ packets it wants to intercept.

Looking at figure 2 above, node “S” wants to send data to node “D”, the destination node. It first initiates the route discovery process. The malicious node “M” immediately sends a response to source “S”, when it receives the route request. If the reply from node “M” reaches the source first, then the source node “S” ignores all other reply messages, and sends packet via route node “M”. As a result, all data packets are consumed, or lost to malicious node. This can lead to a security breach of confidentiality, integrity, and availability.

So, by implication, in black-hole attack, a malicious node uses its routing protocol to advertise itself as having the shortest path to the destination node, or to the packet it wants to intercept the network packets [17].

2.6 Types of Black-hole Attack

There are two types of black-hole attacks described in ad hoc on-demand vector routing protocols (AODV in order). These are internal and external black-hole attacks.

2.6.1 Internal Black-hole attack

In this type of black-hole attack an internal malicious node fits itself in between the routes of a given source, and destination, as shown in figure 3b below. As soon as it gets the chance, this malicious node makes itself an active data route element [17]. At this stage, it gains the capability of conducting attacks against the network. This is an internal attack, because the node itself, at this point, belongs to the data route. Internal attack is more vulnerable to defend, because of difficulty in detecting the internal misbehaving node.

2.6.2 External Black-hole attack

In the case of external black-hole attacks, a malicious node simply stays outside of the network, and denies access to
network traffic, or creates congestion in the network, or disrupts the entire network. External attack can become a kind of internal attack, when it takes control of a legitimate internal node and controls it maliciously to attack other nodes in MANets. The figure 3a below demonstrates an external black-hole attack.

![Figure 3: External and internal attacks [17]](image)

### 2.7 Effects of Black-hole Attack on MANets

The cost of security breach in information communication cannot only be measured in monetary terms, because the reputation, integrity of organizations, and even the lives of its staff, could also be at risk. This is so, because in the event of security compromise, following a Black-hole attack, all three fundamental components confidentiality, integrity, and availability, which make up information security are violated. Black hole attack creates an artificial packet end-to-end delay, by misleading the source node into discarding responses from the legitimate node, while on the other hand keeping the legitimate node waiting for a response. This could have negative implications on bandwidth, and overall network performance. Throughput is also affect since it depends on the real time data being transmitted through the network. In a simulated experiment by [17], it was shown that throughput is higher in the absence of black-hole attack. [17] also highlights that e of data transmitted through the network, is a function of the number of nodes. Therefore, the presence of an illegitimate node adds to the existing network load. In addition, in order to frustrate the entire network, the malicious node tries to intercept all other messages within the network, thereby consuming more bandwidth.

### 3 Related work

#### 3.1 Security techniques in MANets

Security always implies the identification of potential attacks, threats, and vulnerabilities of a certain system. In information systems, security is often defined in the context of being able to ensure confidentiality, integrity, and availability of network resources [18]. This fundamental requirement of computer security, as stated above is also valid when protection of correct routing behavior is to be considered, in any type of network [19]. This section surveys some security schemes, which have been deployed, or proposed to deal, with the attacks described in the earlier sections.

#### 3.2 Wired Equivalent Privacy (WEP)

The security system in WLANS, based on 802.11 standard, consists of a data encapsulation technique called wired equivalent privacy (WEP), and an authentication algorithm called shared key authentication [19]. The weakness of WEP algorithm is that it can easily be broken. Introduced as part of the original 802.11 standard ratified, it was intended to provide data confidentiality, comparable to that of a traditional wired network. WEP, recognizable by 10 or 26 hexadecimal digits, was at one time widely in use, and often the first security choice presented to users by router configuration tools, but it has been observed to have several problems identified with 802.11 securities.

#### 3.3 Watchdog and Pathrater Techniques

The Watchdog and Pathrater technique were introduced by [20] to improve throughput in a MANets, by identifying misbehaving nodes, which trick other nodes, by agreeing to forward the packets without ever doing so. The security model is made up of two components, the watchdog and Pathrater. While the watchdog is used to identify misbehaving (malicious) nodes, initiated by a Replica server, Pathrater helps routing protocols avoid these nodes, by removing them, and creating a new path. The watchdog occurs in every node in the network. When a node forwards a packet, the nodes watchdog component verifies that the next node in the path also forward the packet. The only way a watchdog can do this, is by listening in a promiscuous mode, to the next node’s transmission. If the next node does not forward the packet, it is said to be a malicious (mischievous) node, and has to be reported. This is done by sending an alarm message to the other nodes on its friends list. When the nodes accept the alarm message, they check it, and change the status of the accused node, only if the alarm source is trusted, or a number of trusted nodes accused the same node. The previous status of the node is also maintained, where its structure contains server node ID, destination node ID, hop count and drop packets.

#### 3.4 Intrusion Detection and Response Mechanism (IDRM)

IDRM security model for MANets [21] was first presented by Zhang and Lee. In its architecture, all the nodes take part in the intrusion detection, and response mechanism. Zhang and Lee worked with the basic assumption, that the user and associated program activities are observable, and under a cooperative distributed system. The intrusion detection and response mechanism, by [21] comprised two key modules – a data collector and local detector. The data collection mechanism present in every node, gathers streams of real-time audit data, from various
4. The Design of the Radical Watchdog and Pathrater Algorithm

4.1 Overview of RWP algorithm

The Radical Watchdog and Pathrater algorithm (RWP) is a hybrid technique built on the ideas of Watchdog and Pathrater algorithm introduced by [20]. The RWP is achieved by extending the capabilities of the Watchdog and Pathrater to including a radical deletion of the malicious nodes up to the second hop in the network. The watchdog component on the malicious node detects the misbehaviour of node and then sends warning signals to its neighbouring nodes including the source node. On receiving this signal the source node stops using the malicious node as the link to its destination. All the first hop nodes including the source node delete the malicious node from their friends list and further send the warning signal to the second hop nodes. The second hope nodes respond by flagging the malicious node for future data transactions with it. Any attempt by the malicious node to send RREQ will be met with denial of access and deleted from the friends list. Once the deleted, a warning signal is sent to the next hop. The process will continue until the node is certified as clean by the watchdog component, the watchdog sends a clearance certificate to all its neighbouring nodes causing all the nodes to unflag the malicious node.

4.2 Radical Watchdog and Pathrater algorithm

The algorithm steps of the RWP are:

1. Source node sends route request (RREQ)
2. Node with shortest route sends a (RREP)
3. Watchdog detects that the Node is malicious
4. Watchdog sends an alarm message to the other nodes in first hop
5. Source node stops sending packets to malicious node
6. The nodes receiving the alarm delete the malicious node from friend list
7. And forward the alarm to the second hop nodes
8. On receiving the alert, those nodes on the second hop flag the malicious node, for future reference
9. Any request coming from the flagged node is not entertained and the node is deleted from the friends list, and further warning is send to the next hop nodes
10. Re-integrate the node when Watchdog sends a clearance certificate the node.

4.3 The Sequence diagram

![Sequence diagram for Radical Watchdog and Pathrater](image)

Figure 4: Sequence diagram for Radical Watchdog and Pathrater

The sequence diagram in figure 4 above shows the interaction between objects in the sequential order. The node interaction, passing of messages and relevant alert signals is shown on the sequence diagram.

5. Conclusions and recommendations

Black-hole attack is one of the biggest concerns in Mobile Ad-hoc networks. It violates confidentiality, integrity, and availability; being the important three main components of information security. Black-hole attacks have a negative effect on the networks bandwidth, and the overall network performance is affected by the malicious nodes delaying the packets. The network throughput is reduced significantly. A number of researchers have made enormous contribution towards Black hole detection and elimination. It is hoped that the RWP algorithm presented in this paper adds to the list of techniques to handle the Black hole attack in MANets. RWP is an extension of the WP algorithm presented [20]. RWP algorithm is for detecting and eliminating the black-hole attacks in MANets. It controls the intrusion by the malicious node by deleting and sending warning alerts up to the second hop nodes. This extension ensures that the malicious node is eliminated not only within its surroundings but further across the hops in the mobile ad hoc network. Indications are that the RWP algorithm is an improved algorithm compared to the WP algorithm. Such claims need to be tested through simulation experiments.
Reference


