Enhancing a Network Coding Security Scheme to Prevent Packet Dropping in Wireless Mesh Networks

H.L.H.C. Terblanche and M.J. Grobler
School of Electrical, Electronic and Computer Engineering
North-West University, Potchefstroom Campus
Tel: +27 18 299 1961, Fax: +27 18 299 1977
Email: {20569807, leenta.grobler}@nwu.ac.za

Abstract—Wireless Mesh Networks (WMNs) are the networks that holds the most potential for practical wireless networks of the future [1]. Network Coding (NC) works especially well in WMNs because of their broadcast feature. The nature of WMNs creates a security risk, because there are no control measures. We present a NC security scheme based on [2] for WMNs. The scheme, that already addresses packet pollution attacks, will be enhanced to also address packet dropping in the network. The decrease in packet dropping will cause a decrease in delay and an increase in the efficiency and robustness of the network.

Index Terms—network coding, packet dropping, security, wireless mesh network

I. INTRODUCTION

Wireless Mesh Networks (WMNs) are wireless networks that dynamically form into a mesh topology. Network Coding (NC) works especially well in WMNs because of their broadcast and opportunistic listening properties. NC is a technique where different packets in a network are mixed together and sent through the network to increase the throughput. Authentication is difficult to control in a WMN, because the network forms dynamically, meaning the nodes can randomly join and leave. For example, if a rogue node enters the system undetected, and decides to drop all the packets it receives, those packets are lost.

Packet dropping in WMNs is a security threat that has not been addressed in previous security schemes because they only focussed on packet pollution. Packet dropping can cause a decrease in the efficiency and the throughput, as well as an increase in the delay of the network. If these rogue nodes can be identified and left out of the network, packet dropping can be reduced. By taking a security scheme that focusses on packet pollution and extending it to incorporate packet dropping, a better security scheme can be constructed. The DART [2] security scheme was selected to be adapted, because it does not add as much network overhead as other schemes. Adding too much overhead in a security scheme can diminish the advantages of NC.

In section II background will be given on WMNs, NC, security in NC and the DART security scheme. In section III the proposed research goals and objectives will be given, while in section IV the methodology that will be followed is outlined and the paper concludes in section V.

II. BACKGROUND

A. Wireless Mesh Networks

A WMN is an ad-hoc network that consists of mesh clients and routers that can double as gateways. The nodes in the network dynamically configure themselves into a mesh topology as seen in Fig.1. The network can be static but in most cases is dynamic. The advantages of WMNs are robustness, reliable service coverage, easy network maintenance and low installation costs. These attributes make WMNs a more attractive choice for wireless networks in the future. [1]

B. Network Coding

NC is a technique that optimises the throughput of a network by combining the received packets and sending these combined packets on to the next node. NC was first proposed in [3]. NC works especially well in WMNs because of the network's broadcast feature. The advantages of NC are that it increases the efficiency, maximises the throughput, minimizes the delay, and improves network robustness [4], [5].

C. Security in Network Coding

Secure NC was introduced in 2002 by [6]. There are numerous schemes proposed for security purposes ( [7]–[9]) but by adding the additional security overhead the throughput advantage gained by NC is severely diminished. Current
solutions for security in NC are focused on only three of the five security services [10] namely: message confidentiality, message integrity [8], [11] and message authentication [11]. NC can be divided into two sections: inter-flow NC and intra-flow NC. Inter-flow NC mixes packets across different generations or flows while intra-flow NC mixes packets within the same generation. A generation is a group of packets that are sent in the same time frame. There are various security threats in WMNs [12]. For intra-flow NC the threats are:

- Link quality falsification or modification;
- Wormholes;
- Packet pollution;
- Packet dropping;
- ACK injection or modification;
- ACK dropping;
- ACK delay.

Most of the schemes focus on packet pollution and do not take any of the other security vulnerabilities into account. Packet dropping in WMNs is a security threat, because it decreases the efficiency and increases the delay of the network.

D. DART Security scheme

The DART security scheme was proposed by [2]. The scheme was designed for intra-flow NC in WMNs and addresses packet pollution in WMNs. The scheme is based on time asymmetry and checksums. It claims to have much less overhead than other proposed security schemes. The scheme can be improved by enhancing it to incorporate packet dropping prevention.

III. PROPOSED RESEARCH

The objective of this research is to enhance the DART NC security scheme to prevent packet dropping in WMNs. The research has the following sub-objectives:

- To implement the DART scheme that was proposed in [2];
- To replicate the scheme in GloMoSim and OPNET to compare the results;
- To enhance the scheme for packet dropping prevention.

IV. METHODOLOGY

A Literature survey was done on NC and security in NC. The methodology for further research is as follows:

Literature Study - A literature study will be done on packet dropping in WMNs and on other existing NC security schemes’ advantages, disadvantages and shortcomings.

Analysing the scheme - An analysis of the DART security scheme will be done to understand how it works and how it was implemented.

Implementation in GloMoSim and OPNET - The DART security scheme will be implemented in GloMoSim and compared to the original results to verify that the scheme was implemented correctly. It will then also be implemented in OPNET.

Comparison of results - The results from the different implementations will be compared and analysed.

Enhancing the scheme - The packet dropping prevention will be included in the scheme.

Implementation of enhanced scheme - The enhanced scheme will be implemented again and the results will be compared.

Discussion of results - The results of the different implementations will be analysed and a conclusion will be drawn.

V. CONCLUSION

In this paper it is proposed to take an existing NC security scheme and enhance it to incorporate packet dropping prevention in WMNs. Background was provided to motivate the research and a methodology was presented, to enhance the security scheme. Future work will include implementations and results of the DART scheme.

VI. ACKNOWLEDGEMENTS

This work was completed with funding from the Telkom Centre of Excellence at the NWU, Potchefstroom Campus.

REFERENCES


H.L.H.C. Terblanche is a Telkom CoE student studying for a Masters degree in Computer and Electronic Engineering at the NWU. She received her B.Eng in Computer and Electronic Engineering in 2010 from the NWU. Her current research interests are wireless mesh networks, network coding and security.