Packet Dropping Counter Measures in a MANET Through Reliable Routing Protocol Leveraging a Trust Management Framework

Shirina Samreen, Anurag Group of Institutions, Hyderabad, India

ABSTRACT

The applications of a mobile ad hoc network (MANET) range from military and disaster response to commercial and civilian environments. The intrinsic characteristics like lack of infrastructure, self-organizing nature and deployment flexibility contributes to its usefulness but few other features like open media for communication and topological changes on-the-fly makes it vulnerable to security attacks. The focus of the current work is security mechanisms for a MANET against the various insider attacks targeting the data forwarding operations. It is accomplished through a trust management framework and a secure routing protocol relying upon the TMF to form the routes with most trusted nodes. The protocol computes a novel reliability metric termed as Path Allegiance metric (PAM) which acts as a selection criteria for route selection. The performance evaluation involves simulation results which prove the robustness of the proposed TMF and the effectiveness of the PAM routing protocol in reliable data delivery in the presence of packet droppers which disrupt the data transmission.

KEYWORDS

AODV, AOMDV, AOTMDV, Dempster Shafer Theory, Jousselme Distance, Mobile Ad Hoc Network, Path Allegiance Metric, Security Attacks, Trust Based Routing, Trust Management Framework, Uncertainty Reasoning

1. INTRODUCTION

Since the evolution of wireless technologies and mobile computing hardware, a mobile ad hoc network (MANET) finds extensive usage in many distributed applications. Specifically, many military and disaster response applications deploy a MANET owing to its intrinsic features of no infrastructure requirement, deployment ease and self-organizing nature which contribute to its applicability. Certain other characteristics which include open communication medium involving wire-less links, dynamic signal strength changes causing data transmission fluctuations, dynamic changes in network topology causing broken links due to node mobility and constrained battery power of mobile nodes act as limitations to its applicability and contribute to the security vulnerabilities. Hence the importance associated with its applications along with the vulnerabilities demand a lot of research towards security in MANET and a considerable amount of research has been done already in this field.

A classification of attacks upon MANET based upon the location of the adversary is: Insider attacks and Outsider attacks. The former category of attacks comes up due to the fact that,
communication in a MANET happening in multi-hop fashion and latter category arises due to the existence of open wireless medium.

Another possible classification of attacks upon MANET based upon the network elements which experience the impact is: Control plane attacks and Data plane attacks. The former category of attacks has the routing protocol operation as their target whereas the latter category of attacks has the forwarding decisions employed during data transmission as their target. Accordingly, the focus areas of the security mechanisms designed for MANET can be addressing either the control plane or the data plane.

The focus of proposed security mechanism is over the data plane. It is accomplished through a novel uncertainty reasoning-based trust management framework (TMF) and the application of the TMF in the design of a routing protocol to determine a secure route intending for a reliable data transmission from the source to destination. The route established involves the intermediate nodes with best packet forwarding behaviour which is represented by a quantitative metric known as path allegiance metric (PAM). A reinforcement learning approach is employed wherein the non-malicious nodes perform forwarding actions so as to maximize cumulative reward in the form of improved trust throughout the network. Each forwarding action causes a trust update of a node by some of its peers and the updated trust values at the end of a session are utilized to select the path with the highest path allegiance metric. The path allegiance metric for each path is computed during the route discovery phase through the trust metric values of the nodes computed during the earlier sessions.

The paper is organized as follows to appropriately address the different aspects of the research problem. Section 1 presents the introduction including the objectives of the proposed research. Literature survey is presented by section 2 followed by section 3 which provides the contributions of the research work including the design of the trust management framework, trust components computation mechanisms, and the design of the path allegiance metric-based routing protocol. The performance evaluation is provided in section 4 and followed by the presentation of the conclusions and future enhancements in section 5.

1.1 Objectives

The following objectives are associated with the proposed security solution:

1.1.1. Trust Management Framework Design

The proposed security solution incorporates a TMF which accurately assesses a node’s behavior despite the uncertainty involved in a MANET environment. The behavioral assessment of neighborhood does not rely on promiscuous monitoring; instead an approach employing acknowledgements is used termed as Session Acknowledgement Report (SAR). It facilitates in the behavioral monitoring of only the immediate one-hop neighbors but also the multi-hop non-neighbors based upon evidential proof in the form of SAR packets. This speeds up the trust convergence through direct observations and also reduces the dependency upon recommendations obtained from other neighbor nodes. As a MANET is intrinsically associated with a dynamically changing network topology, it is not possible to eliminate the dependency upon recommendations. Thus, the proposed TMF employs direct as well as indirect trust computed using the recommendations, but the extent of dependency upon recommendations is decreased significantly by having the design of the routing protocol incorporating a condition that, recommendations in trust evaluation should be employed under specific circumstances, when the evaluating node’s uncertainty upon the subject node is greater than a specified threshold.

1.1.2. Design of a Secure Routing Protocol Leveraging the TMF

The TMF proposed in the current research is utilized in the design of a reliable routing protocol. It facilitates in the establishment of route avoiding the nodes which act as malicious packet droppers identified by a low trust metric. A novel reliability measure called as Path Allegiance metric (PAM) is computed to assess the reliability of a path. Following are the features of the PAM routing protocol:
Context-Aware Mobile Capture and Sharing of Video Clips
[www.igi-global.com/chapter/context-aware-mobile-capture-sharing/26571?camid=4v1a](www.igi-global.com/chapter/context-aware-mobile-capture-sharing/26571?camid=4v1a)

Improving Throughput of Starved TCP Flow by Sidestepping Bottleneck Nodes Using Concurrent Transmission
[www.igi-global.com/article/improving-throughput-starved-tcp-flow/40981?camid=4v1a](www.igi-global.com/article/improving-throughput-starved-tcp-flow/40981?camid=4v1a)