RESEARCH ARTICLE OPEN ACCESS

# Protected High Throughput Multicast Routing Wireless Mesh Network

Karthik P[1], Arivazhagi P[2]

1(Assistant Professor, Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and Thanjavur)

2 (M.C.A., Scholar Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and Thanjavur)

## Abstract:

Multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously. We identify novel attacks against high-throughput multicast protocols in wireless mesh networks. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic. We show that these attacks are very effective against multicast protocols based on high-throughput metrics. We conclude that aggressive path selection is a double-edged sword: While it maximizes throughput, it also increases attack effectiveness in the absence of defense mechanisms. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks. We demonstrate both the attacks and our defense using ODMRP, a representative multicast protocol for wireless mesh networks, and SPP, an adaptation of the well-known ETX unicast metric to the multicast setting.

***Keywords*** — networks, attacks, protocols, ODMRP, defense, .

## I. INTRODUCTION

This Wireless mesh networks (WMNs) emerged as a promising technology that offers low-cost high-bandwidth community wireless services. A WMN consists of a set of stationary wireless routers that form a multi-hop backbone, and a set of mobile clients that communicate via the wireless backbone. Numerous applications envisioned to be deployed in WMNs, such as webcast, distance learning, online games, video conferencing, and multimedia broadcasting, follow a pattern where one or more sources disseminate data to a group of changing receivers. These applications can benefit from the service provided by multicast routing protocols.

Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. In the last few years, several protocols were proposed to provide multicast services for multi-hop wireless networks. Initially, these protocols were proposed for mobile ad hoc networks, focusing primarily on network connectivity and using the number of hops (or hop count) between the source and receivers as the route selection metric. However, many of the applications that benefit from multicast services also have high-

throughput requirements, and hop count does not maximize throughput as it does not take into account link quality. Given the stationary nature and increased capabilities of nodes in mesh networks, recent protocols focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links. We refer to such metrics as link-quality metrics or high-throughput metrics, and to protocols using such metrics as high-throughput protocols.

In a typical high-throughput multicast protocol, nodes periodically send probes to their neighbors to measure the quality of the links from their neighbors. During route discovery, a node estimates the cost of the path by combining its own measured metric of adjacent links with the route cost accumulated on the route discovery packet. The path with the best metric is then selected. High-throughput metrics protocols require the nodes to collaborate in order to derive the path metric, thus relying on the assumption that nodes are collaborative and behave correctly during metric computation and propagation.

## II. PROBLEM ANALYSIS

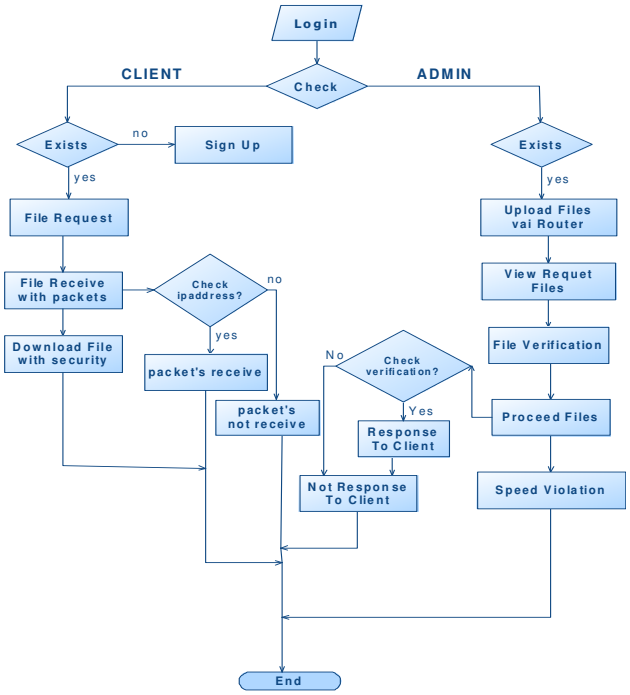
Previous work showed vulnerabilities of unicast routing protocols that use hop count as a metric. Several unicast routing protocols were proposed to cope with outsider or insider attacks. Secure wireless multicast was less studied and focused primarily on tree-based protocols using hop count as a path selection metric. Hence, we make the observation that defense mechanisms cannot rely on the existing metric for recovery and have to either resort to a fallback procedure not using the metric or refresh the metric before starting recovery.

### *A. Issues*

- Path selection is based on the greedy approach of selecting path with best metric (e.g., highest SPP, lowest latency).
- An estimation of the target performance metric can be derived from the path metric.
- There exists an efficient metric refreshment protocol that allows nodes to obtain correct metrics for attack recovery. Such metric refreshment can be easily achieved by flooding of a new metric establishment message.

## III. PROPOSED METHODOLOGY

Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks. We proposed to provide multicast services for multi-hop wireless networks. Initially, these protocols were proposed for mobile ad hoc networks (MANETs), focusing primarily on network connectivity and using the number of hops (or hop count) between the source and receivers as the route selection metric. However, many of the applications that benefit from multicast services also have high-throughput requirements, and hop count does not maximize throughput as it does not take into account link quality. Given the stationary nature and increased capabilities of nodes in mesh networks.



### A. *Advantages*

*I)* We propose a defense scheme that combines measurement -based detection and accusation-based reaction techniques.

*II)* To accommodate transient network variations, we use temporary accusations that have duration proportional to the disruption created by the accused node.

*III)* To prevent attackers from exploiting the defense mechanism itself, we limit the number of accusations that can be generated by a node.

*IV)* We perform a detailed security analysis of our defense scheme and establish bounds on the impact of attacks.

## III. MODULES DESCRIPTION

### A. *NETWORK MODEL*

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

### B. *RSA KEY GENERATION*

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, We use RSA signatures with 1024-bit keys, simulating delays to approximate the performance of a 1.3 GHz Intel Centrino processor. We empirically tune the threshold _ = 20% to accommodate random network variations in the simulated scenarios. The timeout for React Timer is set as 20(1−ePDR) millisecond, and the accusation time is set as 250(ePDR−pPDR) second. Nodes use the statistical-based method described in Sec. IV-C2 to determine their pPDR.Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N.[3] specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

### C. *DIGITAL SIGNATURE (SENDING PACKETS)*

Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

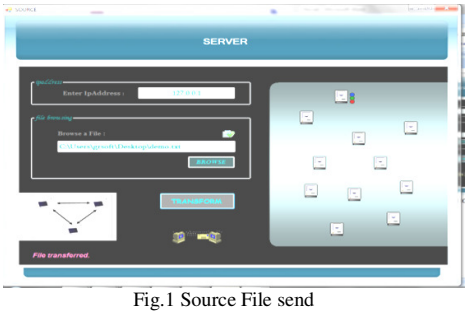



Fig.1 Source File send

### D. *SIGNATURE VERIFICATION (RECEIVING PACKETS)*

Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient.The intended recipient (or any other party) verifies the

signature to determine its authenticity. Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory's public key and identity shall be made available to the verifier in an authenticated manner. The public key may, for example, be obtained in the form of a certificate signed by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner.

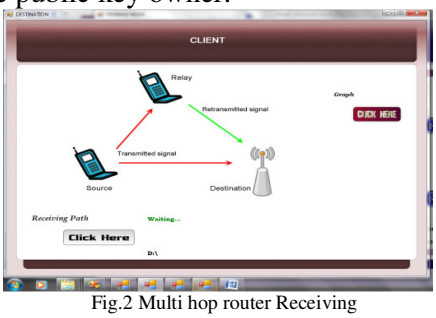



Fig.2 Multi hop router Receiving

### *E. ODMRP PROTOCOL*

We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. Below we first give an overview of ODMRP, then describe how it can be enhanced with any link-quality metric. The protocol extension to use a high-throughput metric was first described by Roy et al. We refer to the ODMRP protocol using a high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP protocol.

ODMRP is an on-demand multicast routing protocol for multi-hop wireless networks, which uses a mesh of nodes for each multicast group. Nodes are added to the mesh through a route selection and activation protocol. The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and update the routes. We use the term round to denote the interval between two consecutive mesh creation events. JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message.

## IV. ACCOMPLISHMENT

Implementation is the stage where the theoretical is converted into a working system. This is the process of converting a new or a revised system into an operational one of the implementation consists of

Testing the developed system with sampled data.

- Detection and correction of errors.
- Making necessary charges in the system.
- Checking of reports with that of the existing system.
- Training of hardware and software utilities.
- Installation of hardware and software utilities.

The implementation of the system is easy for any system environment, as the software used is portable one.

### *A. Key in Design*

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system.

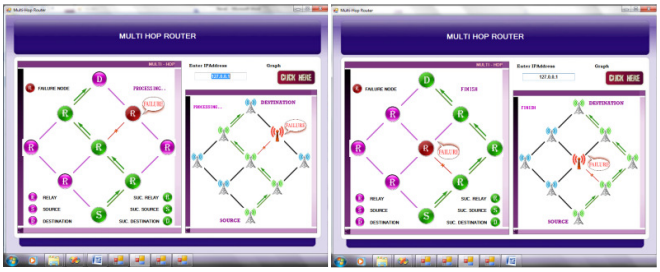



Fig.3 Multi hop router Receiving

The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

**Objectives**

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

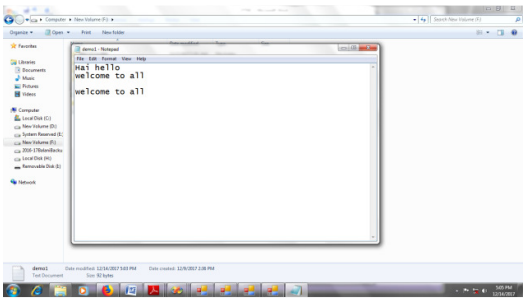



Fig.4Receiving file status

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

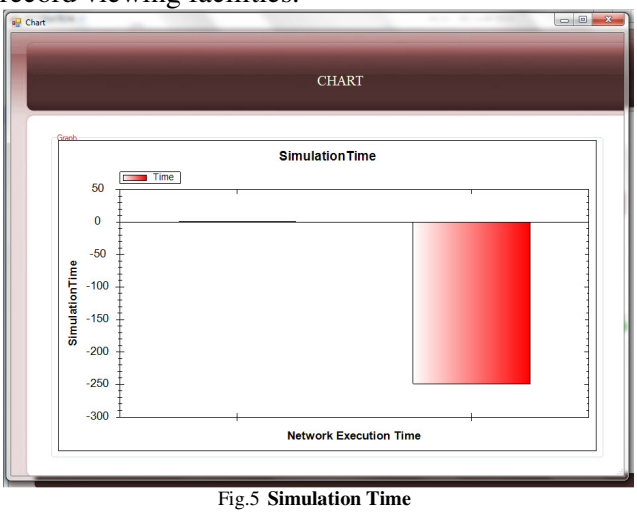



Fig.5 **Simulation Time**

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

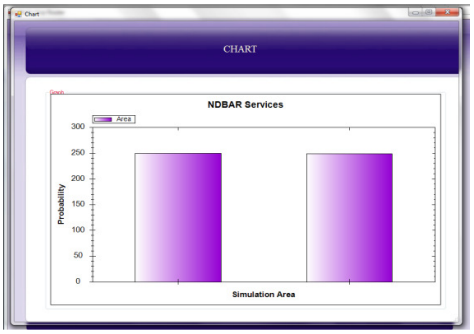



Fig.6 **Novel Network Service**

***B. Key Output Design***

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

**V. CONCLUSION**

This project considered the security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, we identified metric manipulation attacks that can inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect. overcome the challenges with our novel defense scheme that combines measurement-based attack detection and accusation-based reaction. Our defense also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. In demonstrate through experiments that our defense is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead.

### *A. IMPROVEMENT*

- Solve the hidden-terminal problem, which is really a question of coordinating a large number of radios to reduce interference.
- Coordinate individual radios so that Quality of Service can be guaranteed in a mesh network.
- Reduce power consumption of the entire system, especially user devices.
- Create standard ad hoc routing and MAC layers that work for large meshed networks of mobile nodes with high throughput and low delay over many hops.

## REFERENCES


1. I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, vol. 47, no. 4, pp. 445–487, 2005.
2. P. A. K. Acharya and E. M. Belding, "MARS: link-layer rate selection for multicast transmissions in wireless mesh networks," Ad Hoc Networks, vol. 9, no. 1, pp. 48–60, 2011.
3. N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, "Wireless mesh networks: current challenges and future directions of web-in-the-sky," IEEE Wireless Communications, vol. 14, no. 4, pp. 79–89, 2007.
4. S. Paul, Multicast on the Internet and Its Applications, Kluwer Academic, New York, NY, USA, 1998.
5. M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proceedings of the ACM Workshop on Wireless Security (WiSE'02), pp. 1–10, Atlanta , Ga, USA, September 2002
6. R. Matam and S. Tripathy, "Improved heuristics for multicast routing in wireless mesh networks," Wireless Networks, vol. 19, no. 8, pp. 1829–1837, 2013.
7. T. R. Andel and A. Yasinsac, "Adaptive threat modeling for secure Ad Hoc routing protocols," Electronic Notes inTheoretical Computer Science, vol. 197, no. 2, pp. 3–14, 2008.
8. R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," International Journal of Network Security, vol. 16, no. 3, pp. 168–178, 2014.
9. M. Burmester and B. D. Medeiros, "Towards provable security for route discovery protocols in mobile ad hoc networks," IACR Cryptology ePrint Archive, 2007.
10. G. Acs, L. Butty ´ an, and I. Vajda, "Provable security of on- ´ demand distance vector routing in wireless ad hoc networks," in Security and Privacy in Ad-Hoc and Sensor Networks, R. Molva, G. Tsudik, and D. Westhoff, Eds., vol. 3813 of Lecture Notes in Computer Science, pp. 113–127, 2005.
11. L. Mao and J. Ma, "Towards provably secure on-demand distance vector routing in MANET," in Proceedings of the International Conference on Computational Intelligence and Security (CIS '08), pp. 417–420, Suzhou, China, December 2008.