SECURE-ON DEMAND MULTICAST ROUTING IN WIRELESS MESH NETWORKS

Ms. M.Malathy[1], Ms. D. Mary Ponrani[2]
[1, 2] Assistant Professor, CSE, Dr. Sivanthi Aditanar College of Engineering,
Tiruchendur, Tamilnadu, (India)

ABSTRACT

Recent work in 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. In this work, 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 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—Wireless Mesh Networks, High-Throughput Metrics, Secure Multicast Routing, Metric Manipulation Attacks, Byzantine Attacks.

I. INTRODUCTION

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 multihop 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 multihop wireless networks. These protocols were proposed for mobile ad hoc networks (MANETs), focusing primarily on network connectivity and using the number of hops (or hop count) as the route selection metric. However, it has been shown that using hop count as routing metric can result in selecting links with poor quality on the path, negatively impacting the path throughput. Instead, given the stationary nature of WMNs, recent protocols focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links .I 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 their adjacent links. During route discovery, a node estimates the cost of the path by combining its own measured metric of adjacent links with the path cost accumulated on the route discovery packet. The path with the best metric is then selected. High-throughput protocols require the nodes to collaborate in order to derive the path metric, thus relying on the assumption that nodes behave correctly during metric computation and propagation. However, this assumption is difficult to guarantee in wireless networks that are vulnerable to attacks coming from both insiders and outsiders, due to the open and shared nature of the medium and the multihop characteristic of the communication. An aggressive path selection introduces new vulnerabilities and provides the attacker with an increased arsenal of attacks leading to unexpected consequences. For example, adversaries may manipulate the metrics in order to be selected on more paths and to draw more traffic, creating opportunities for attacks such as data dropping, mesh partitioning, or traffic analysis.

II. RELATED WORK

2.1 TITLE: A Secure Routing Protocol for Ad Hoc Network. AUTHORS: K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields.

Most recent ad hoc network research has focused on providing routing services without considering security. In this paper, we detail security threats against ad hoc routing protocols, specifically examining AODV and DSR. In light of these threats, we identify three different environments with distinct security requirements. They propose a solution to one, the managed-open scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected. This protocol, ARAN, is based on certificates and successfully defeats all identified attacks.

2.2 TITLE: Secure Link State Routing for Mobile Ad Hoc Networks. AUTHORS: P. Papadimitratos and Z.J. Haas

The secure operation of the routing protocol is one of the major challenges to be met for the proliferation of the Mobile Ad hoc Networking (MANET) paradigm. Nevertheless, security enhancements have been proposed mostly for reactive MANET protocols. The proposed here Secure Link State Routing Protocol (SLSP) provides secure proactive topology discovery, which can be multiply beneficial to the network operation. SLSP can be employed as a stand-alone protocol, or fit naturally into a hybrid routing framework, when combined with a reactive protocol. SLSP is robust against individual attackers, it is capable of adjusting its scope between local and network-wide topology discovery, and it is capable of operating in networks of frequently changing topology and membership.

2.3 TITLE: Secure Neighbor Discovery in Wireless Networks Formal Investigation of Possibility. AUTHORS: M. Poturalski, P. Papadimitratos, and J.-P. Hubaux

Wireless communication enables a broad spectrum of applications, ranging from commodity to tactical systems. Neighbor discovery (ND), that is, determining which devices are within direct radio communication, is a building block of network protocols and applications, and its vulnerability can severely compromise their functionalities. A number of proposals to secure ND have been published, but none have analyzed the problem formally. In this paper, they contribute such an analysis: They build a formal model capturing salient characteristics of wireless systems, most notably obstacles and interference, and we provide a specification of a basic variant of the ND problem. Then, they derive an impossibility result for a general class of protocols we term time-based protocols," to which many of the schemes in the literature belong. They also identified the conditions under which the impossibility result is lifted. Moreover, they explore a second class of protocols termed time- and location-based protocols," and prove they can secure ND.

2.4 TITLE: Detecting the Sybil Attack in Mobile Ad hoc Networks. AUTHORS: C. Piro, C. Shields, and B.N. Levine

Mobility is often a problem for providing security services in ad hoc networks. In this paper, they showed that mobility can be used to enhance security. Specifically, they showed that nodes that passively monitor traffic in the network can detect a Sybil attacker that uses a number of network identities simultaneously. They showed through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. They then showed that although the detection mechanism will falsely identify groups of nodes traveling together as a Sybil attacker, they can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes traveling in close proximity.

2.5 TITLE: A Protocol for Geocasting in Mobile Ad Hoc Network. AUTHORS: Y.-B. Ko and N.H. Vaidya,

Consider the problem of providing a geocast service in mobile ad hoc networks and presents a novel Geocasting algorithm combining unicasting and flooding. Geocast is useful for sending messages to everyone in a specified geographical region. The proposed protocol is named GeoTORA, because it is derived from the TORA (unicast) routing protocol. Flooding is also incorporated in GeoTORA, but it is limited to nodes within a small region. This integration of TORA and flooding can significantly reduce the overhead of geocast delivery, while maintaining reasonably high accuracy.

III. THE PROPOSED SYSTEM

I propose a secure high-throughput multicast protocol S-ODMRP that incorporates a novel defense scheme Rate Guard. Rate Guard combines measurement based detection and accusation based reaction technique to address the metric manipulation and packet dropping attacks.

3.1 Mesh Creation

S-ODMRP mesh creation follows the same pattern of ODMRP-HT. The source node S periodically broadcasts to the entire network a JOIN QUERY message in order to refresh the membership information and to update the routes. The JOIN QUERY message is signed by S and is propagated using a weighted flood suppression mechanism. Nodes only process JOIN QUERY messages that have valid signatures and that are received from nodes not currently accused (indicated by an ACCUSATION LIST maintained by each node). Nodes record the upstream node and the metric corresponding to the route with the best metric as best upstream and best metric. The JOIN REPLY messages are then sent from receivers back to S along optimal paths as defined by the high throughput metric, leading to the creation of the FORWARDING GROUP (the multicast mesh). After sending a JOIN REPLY to its best upstream, a node starts to monitor the PDR from its best upstream in order to measure its perceived PDR (pPDR).

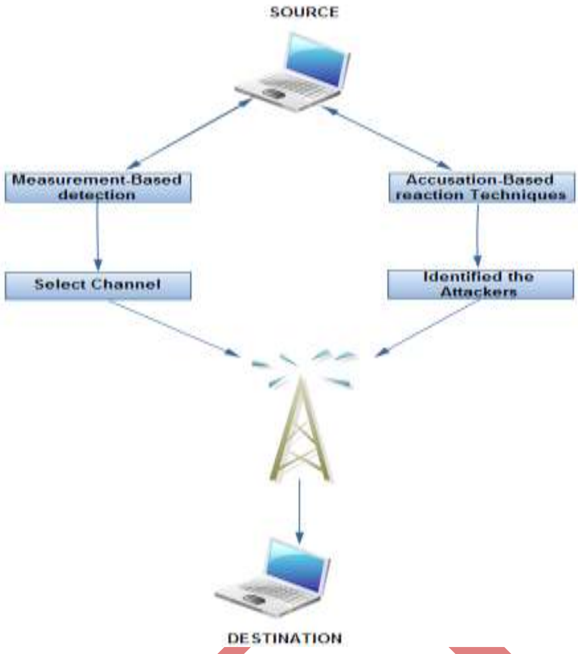
SOURCE
Measurement-Based detection
Accusation-Based reaction Techniques
Select Channel
Identified the Attackers
DESTINATION

Fig 1. Architecture Diagram

3.2 Attack Detection

We detect attacks using a measurement-based mechanism, where each FORWARDING GROUP and receiver node continuously monitors the discrepancy between ePDR and pPDR and flags an attack if ePDR-pPDR .The most straightforward method for estimating pPDR is to use a sliding window method, with pPDR calculated as pPDR ¼ r=w, where r is the number of packets received in the window and w is the number of packets sent by the source (derived from packet sequence numbers) in the window. Albeit being simple, this method is sensitive to bursty packet loss. In addition, this approach requires a node to wait until at least w packets are sent in a round before being able to make any decision. Therefore, setting too large causes delay in making decisions, whereas setting to small results in inaccurate pPDR estimation and hence more frequent false positives. In general, it is difficult to determine the optimal value for w, as it depends on the network conditions and the specific position of a node. To avoid these short comings, I propose an efficient statistical-based estimation method for pPDR that naturally adapts to the network environment of each node.

3.3 Attack Reaction

This protocol uses a controlled-accusation mechanism which consists of three components, staggered reaction time-out, accusation message propagation and handling, and recovery message propagation and handling. When a node detects attack behavior, it starts a React Timer with time-out value ePDR, where is a system parameter that determines the maximum time-out for reaction timer. Since ePDR decreases monotonically along a multicast data path, nodes farther away from the source will have a larger time-out value for the React Timer. This staggered time-out technique ensures nodes immediately below the attacker will take action first, before any of their downstream nodes mistakenly accuse their upstream node. When the React Timer of a node N expires, N accuses its best upstream node and cancels the React Timer at its downstream nodes with the following actions: Create, sign, and flood an ACCUSATION message in the network, which contains N's identity (the accuser node) and the identity of N’s best upstream node (the accused node). The message also contains a value accusation time ePDR-pPDR, indicating the amount of time accusation lasts is a tunable system parameter that determines the severity of attack punishment. Create, sign, and send to its downstream nodes a RECOVERY message, which contains the ACCUSATION message. This message serves the role of canceling React Timer of nodes in N’s sub tree and activating the fallback procedure at the receivers in N’s sub tree. Upon receipt of an ACCUSATION message, a node checks if it does not have an unexpired accusation from the same accuser node and verifies the signature on the message. This enforces limited accusation mechanism, which allows nodes to only have one active accusation at a time. If both checks pass, the node adds a corresponding entry to its ACCUSATION LIST .Accusations are removed from the ACCUSATION LIST after the accusation time has elapsed.

3.4 Fallback Recovery

The accusation mechanism ensures that when the metric is refreshed in the round after the attack detection, the accused nodes are isolated. However, during the round when an attack is detected, the receiver nodes in the sub tree of the attacker need to find alternative routes to “salvage” data for the rest of the round. A side effect of metric manipulation attacks is metric poisoning, which prevents recovery by relying on the metrics in the current round. Address this inability by falling back to the fastest route for routing during the remainder of the round. Specifically, during the JOIN QUERY flooding, besides recording the best upstream node, each node also records the upstream for the fastest route as fastest upstream. To recover from an attack, a receiver sends a special JOIN REPLY message (a salvage message) to its fastest upstream node. Each node on the fastest route forwards the special JOIN REPLY message to their fastest upstream node and becomes part of the FORWARDING GROUP.

3.5 Rate Guard

RateGuard relies on the observation that regardless of the attack strategy, either by dropping JOIN REPLY, metric manipulations, or by dropping packets, attackers do not affect the multicast protocol unless they cause a drop in the packet delivery ratio (PDR).An reactive approach is adopted in which attacker nodes are detected through a measurement- based detection protocol component, and then isolated through an accusation-based reaction protocol component.

3.5.1 Measurement-Based Attack Detection

Whether by packet dropping alone or by combining it with metric manipulation to attract routes, the effect of an attack is that data are not delivered at a rate consistent with the advertised path quality. A generic attack detection strategy is proposed that relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). A node can estimate the ePDR of a route from the value of the metric for that route; the node can determine the pPDR for a route by measuring the rate at which it receives data packets from its upstream on that route. Both FORWARDING GROUP nodes and receiver nodes monitor the pPDR of their upstream node. If ePDR - pPDR for a route becomes larger than a detection threshold ∂, then nodes suspect that the route is under attack because the route failed to deliver data at a rate consistent with its claimed quality.

3.5.2 Accusation-Based Attack Reaction

A controlled accusation mechanism is used in which a node, on detecting malicious behavior, temporarily accuses the suspected node by flooding in the network an ACCUSATION message containing its own identity (the accuser node) and the identity of the accused node, as well as the duration of the accusation. As long as the accusation is valid, metrics advertised by an accused node will be ignored and the node will not be selected as part of the FORWARDING GROUP. This strategy also successfully handles attacks against path establishment. From the downstream node point of view, the dropping of a JOIN REPLY message causes exactly the same effect as the attacker dropping all data packets, thus the downstream nodes will react and accuse the attacker**.**

IV. EXPERIMENTAL RESULTS

Simulation setup: ODMRP-HT and S-ODMRP are implemented using the ODMRP version available in the Glomosim simulator. Nodes use 802.11 radios with 2 Mbps bandwidth and 250 m nominal range. Simulate environments representative of mesh network deployments by using the two-ray radio propagation model with the Rayleigh loss model, which models environments with large reflectors, e.g., trees and buildings, where the receiver is not in the line-of-sight of the sender.

The network consists of 100 nodes randomly placed in a 1; 500 m _ 1; 500 m area. Select 20 nodes randomly as multicast group members and one randomly selected node among them as the data source. Attackers are randomly selected among nodes that are not group members. Group members join the group in the beginning of the simulation. At second 100, the source starts multicasting 512-byte data packets for 400 seconds at a rate of 20 packets/second. For S-ODMRP, RSA signatures are used with 1024-bit keys, simulating delays to approximate the performance of a 1.3 GHz Intel Centrino processor. Empirically tune the threshold ∂= 20% to accommodate random network variations in the simulated scenarios. The time-out for React_Timer is set to 20(1 -ePDR) millisecond (i.e., β= 20) and the accusation_ time is set to 250(ePDR - pPDR) second (i.e. α= 250). Nodes use the statistical-based method described to determine their pPDR.

V. CONCLUSION AND FUTURE WORK

The security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, the metric manipulation attacks is identified 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. The challenges can be overcome with the novel defense scheme, RateGuard that combines measurement-based attack detection and accusation-based reaction. This defense also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. This defense is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead. In S-ODMRP, a node is detected as an attacker only if the PDR drop caused by the node exceeds the threshold ∂.Therefore, this leaves the room for an attacker to drop some amount of data below the threshold ∂ without being detected. Since the threshold ∂ models the normal PDR variation exhibited by legitimate nodes, it is impossible to distinguish such attackers from normal nodes. One may address this shortcoming with more accurate modeling of the behavior of normal nodes. For example, we can incorporate both the mean and the variance of PDR. Since we expect PDR to vary around its mean under normal network variations, a node whose PDR is constantly below its advertised value, even only for a small amount, can be seen as abnormal. Such enhancements are deferred as future work.

REFERENCES

[1] E.L. Madruga and J.J. Garcia-Luna-Aceves, “Scalable Multicasting: the Core-Assisted Mesh Protocol,” Mobile Networks and Applications, vol. 6, no. 2, pp. 151-165, 2001.

[2] S.J. Lee, W. Su, and M. Gerla, “On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks,” Mobile Networks and Applications, vol. 7, no. 6, pp. 441-453, 2002.

[3] E.M. Royer and C.E. Perkins, “Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing,” Internet Draft, July 2000.

[4] J.G. Jetcheva and D.B. Johnson, “Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks,” Proc. ACM MobiHoc, 2001.

[5] S. Roy, V.G. Addada, S. Setia, and S. Jajodia, “Securing MAODV: Attacks and Countermeasures,” Proc. Second Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’05), 2005.

[6] R. Curtmola and C. Nita-Rotaru, “BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-Hop Wireless Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 4, pp. 445-459, Apr. 2009.

[7] A. Perrig, R. Canetti, D. Song, and D. Tygar, “Efficient and Secure Source Authentication for Multicast,” Proc. Network and Distributed System Security Symp. (NDSS), Feb. 2001.