ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

High-Throughput in Wireless Mesh Networks Using Different Routing Metrics

K. Jaya[1], S.Saranya[2], S.Nandhini Devi[3]

M.E CSE II[nd]Year, Srinivasan Engineering of College, Perambalur, India[1]

M.E CSE II[nd]Year, Srinivasan Engineering of College, Perambalur, India[2]

Assistant Professor, Dept. of CSE, Srinivasan Engineering of College, Perambalur, India[3]

ABSTRACT- Wireless Mesh Networks (WMN) can be designed using a routing technique. There is lot of protocols developed for many packets delivery, but they fail in the path selection in the presence of selfish nodes. To overcome this problem, Cross layer metrics is developed which is used to select the path that delivers the highest packet. The Optimized Link State Routing Protocol (OLSR) is used by individual nodes to compute next hop destinations for all nodes in the network.Expected Forwarded Counter (EFW), and two further variants, handle with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMN. EFW selects reliable and high-performance path for packet transmission. The results show that the path reliability and increase the performance of the network.

KEYWORDS: Packet transmission, Routing Metrics, Selfish Nodes, Wireless Mesh Networks.

I. INTRODUCTION

Wireless Mesh Networks (WMNs) have emerged as a technology for next generation wireless networking, fostering the development of new network paradigms such as wireless mesh community networks (WMCNs). Since many applications envisioned to run on WMCNs have high-throughput requirements, recent research has introduced several link layer metrics that capture the quality of wireless links to select the network paths with the highest delivery rates. However, most of these metrics have been considered assuming that each wireless mesh router participates honestly in the forwarding method. This assumption may be valid in a network managed by Network operator, it is not automatically happened in a network where the participants are managed by different entities that may benefit from not forwarding the traffic.

Effectively, in a WMCN, a selfish user that provides connectivity through his own mesh routers might try to greedily consume the available bandwidth by favoring his traffic to the detriment of
others, by selectively dropping the packets sent by other nodes. Tools like *iptables* can be used to easily implement packet dropping at the network layer. The selfish behavior can cause unfairness and severe performance degradation, since periodic dropping the packets at relaying nodes, decreases the throughput of closed loop connections (such as TCP) established by other nodes, when the fraction of dropped packets is less.

Previous works focused mainly on the detection of nodes that exhibit selfish behavior and their exclusion from the network. To the best of our knowledge, only two routing metrics have been proposed in the research literature to consider the selfish behavior of network nodes. These metrics, tailored for reactive routing protocols like AODV and DSR, increase the hop count of a network path proportionally to the number of selfish nodes that belong to that path. However, the hop count and the above cited metrics do not model accurately the wireless link quality. As a result, the community network is left with several link-layer metrics that fail to choose high- throughput paths between a source and a destination in the presence of selfish nodes which drop packets at the network layer.

In this paper propose a cross-layer metric that selects the path with the highest packet delivery rate considering both the quality of wireless links and the reliability of network nodes. While many factors contribute to the earlier, like interference

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

and received signal strength, the latter is mainly influenced by the selfishness of the users that control and manage the network.

Cross-layer metric selects the path with the highest packet delivery rate considering both the quality of wireless links and the reliability of network nodes. While many factors contribute to the earlier, like interference and received signal strength, the final is mainly influenced by the selfishness of the users that control and accomplish the network devices. To design Expected Forwarding Counter (EFW), a new reliability metric that combines information across the routing and MAC layers to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMN. This metric combines direct observation of routing-layer forwarding behavior of neighbors with the MAC-layer quality of wireless links in order to select the most reliable and high-performance path.

Two variants of EFW namely Minimum Expected Forwarding Counter (MEFW) and Joint Expected Forwarding Counter (JEFW), capture the worst and joint dropping behavior of the nodes that have established the wireless link, in order to reduce the complexity of the network topology representation and the signaling overhead.The proposed metrics are loop-free when used to construct a hop-by-hop forwarding scheme based on the Dijikstra's algorithm. It also analyzes the robustness of the three proposed metrics to selfish nodes trying to manipulate the metric computation and show that MEFW is the most robust to such attacks.

II. RELATED WORKS

Several research works deal with reliable data transmission in wireless multi-hop networks with selfish participants. The detection techniques and incentives, which are used to address this problem.The earlier approach deals with detecting the dropping activities and, if necessary, without the embarrassed nodes from the network. ODSBR leverages on an active probing technique to detect unreliable links controlled by adversary nodes, and defines an innovative route discovery mechanism to avoid network paths containing such links. Castor is an opportunistic routing protocol that uses both flooding and unicast transmission techniques to deliver reliably the message to the destination. Sprout is a routing protocol that probabilistically generates a multiplicity of link-disjoint paths to reach other network nodes and deliver messages using the most reliable route.

The secure message transmission (SMT) protocol proposed in exploits multiple node disjoint paths to increase the end-to-end delivery rate using a message spreading scheme that enables the destination to recover the information contained in data packets by increasing its redundancy. All previous solutions measure the path set reliability using an end-to-end acknowledgment mechanism. However, this active detection technique results in an increased network overhead and thus in a lower available bandwidth for data connections.

Other protocols that define a satisfying mechanism to substitute node cooperation are proposed. In wireless committee networks the authors propose a distributed algorithm based on the concept of exchange among nodes, where credit is represented by the amount of traffic directly or indirectly forwarded by other network nodes. In mobile ad-hoc WANs the authors propose two forwarding approaches, the Packet Purse Model (PPM) and the Packet Trade Model (PTM), through which the intermediate nodes trade in packets.

Routing metrics proposed in newest years for wireless multihop networks fail to select the network paths with the highest delivery rate in the presence of intermediate nodes whose forwarding behavior is driven by selfish interests. To overcome this problem, we propose a cross-layer routing metric, EFW, and two alternative refinements, MEFW and JEFW, to select the most reliable path by considering both the quality of wireless links and the forwarding behavior of network nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

III. SYSTEM MODEL

A. Network Model

This paper considers a wireless mesh community network collected of two different types of devices: mesh routers that form the infrastructure of the WMCN and are maintained by different community users, and customer devices that are only interested in the services provided by the WMCN (e.g., Internet access).Since the network architecture has a hierarchical structure (wireless mesh routers are in fact dedicated nodes which are organized to offer backhaul services), to assume the existence of a subset of community participants that are responsible for all management tasks. To undertake that all mesh routers communicate with each other using the wireless medium; in particular, they use the IEEE 802.11 MAC protocol to organize access to the channel. All mesh routers are armed with at least one omni directional antenna for backbone communications.

B. Security Model

Assume that there occurs a public key infrastructure managed by a trusted Certification Authority (CA). For each new mesh router that a community user wants to add to the WMCN, the CA generates a unique public/private key pair and issues a certificate that binds the identity of the mesh router to its public key. The cryptographic keys can be used to implement message authentication schemes similar to those proposed in ad-hoc network, in order to prevent message fake and replay attacks. Additionally, to avoid packet manipulation attacks against data traffic, which may totally affect the performance of closed-loop connections like TCP and need that a secure end-to-end tunnel (like IPSec) recognized between any two devices that communicate with each other through an application layer protocol.

Two different policies can be considered. The first policy The does not discriminate, in the packets forwarded by mesh routers, between traffic created by router owners and traffic of other users and customers, due for instance to higher layer encryption mechanisms. The second policy spoils mesh router owners only for forwarded packets originated by other users and customers. In this case, the user can apply discarding policies only to a subset of the mesh routers in order to harm traffic that contests with the own for some network resources.

Finally, to emphasize that attacks against the routing plane, in which nodes simply ignore some of the procedures clear by the routing protocol, represent an orthogonal concern to the problem considered in this paper, and can be addressed using detection schemes. In the Optimized Link-State Routing protocol (OLSR), individual nodes used to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. Link-state routing protocols such as Open Shortest Path First (OSPF) and elect a designated router on every link to perform flooding of topology information.

IV. PROPOSED SYSTEM

A. Expected Forwarding Counter

The routing algorithm represents the network topology using a directed graph when EFW is used as link metric. Therefore, a selfish node cannot restore the network path on which it lies as best alternative if it's dropping behavior is detected by the previous node on the path. However, the selfish node can easily affect the selection of the reverse path of the connection by conducting a neighbor metric attack.

B. Minimum Expected Forwarding Counter

The MEFW metric is the most robust of the three metrics against neighbor metric attacks. It identifies the selfish node by using the EFW metric in the network. That simplifies the topology representation and captures the worst node. To reduce the complexity of network. To evaluate the effectiveness and the scalability of the proposed metrics through simulations. Expected Forwarding Counter and two variants of solutions considerably increase both the network throughput and fairness

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

with respect to the baseline approach that takes into account only the successful transmission rate of a wireless link. It can be concluded that the proposed metric and its refinements represent an effective solution for achieving highly resilient routing.

C. Joint Expected Forwarding Counter

JEFW is the most vulnerable among the three proposed metrics to neighbor metric attacks since the forwarding rates of both the adjacent nodes are combined to compute the link cost. The problem can be partially addressed by replacing the link quality and the forwarding rate of the neighbor transmitted within the routing message with the product of the two values. In addition to reducing the signaling overhead, this improvement increases the robustness against lying attacks since a selfish node cannot distinguish between the two factors that contribute to the whole link cost.

V. OPTIMIZED LINK STATE ROUTING PROTOCOL

A.Path Selection

Transmit the message to the reciever by selecting the shortest path and high content delivery.Expected forwardding counter combines the information across the routing and MAC layer to handle with problem of selfish behavior of mesh router in a WMN. The metric combines direct observation of routing-layer forwarding behavior of neighbors with the MAC-layer quality of wireless links in order to select the most reliable and high-performance path.

B. Message Transmission

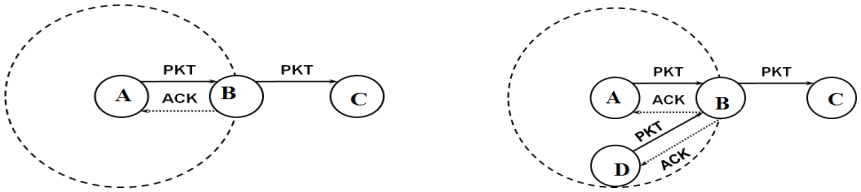
When the user transmit the message,browse a file that needs to send to the destination node.When the data has been received successfully the acknowldegment received to the sender.Router routes the packet to the reciever according to the destination IP address. Minimum Expected Forwarding Counter (MEFW) and Joint Expected Forwarding Counter (JEFW), which capture the worst and joint dropping behavior of the nodes that have established the wireless link, in order to reduce the complexity of the network topology .

C. Exclude Selfish Nodes

When transmit the message the acknowldegment has not been received successfully,it is dropped by selfish nodes in wireless mesh network, ETX measures the expected number of packet transmissions and retransmissions, desired to acceptably send the packet done a wireless link. In order to compute ETX, it is necessary to estimate the packet loss probability in both directions and calculate transmission and retransmission of packets.

D. Forwarding Probability Estimation

The forwarding probability estimation mechanism represents a core component of the entire design, then the range of the best consistent network paths directly depends on its accuracy .The metric selects the path with the highest delivery rate considering the quality of wireless links and the reliability of network nodes.To choose high throughput path in the network.



(X) (Y)

Figure 1: Example of forwarding packet estimation executed by node N 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

To illustrate the forwarding probability estimation performed by a mesh router by referring the example of network scenario shown in Figure 1, where hard and scattered lines denote the transmission of packets and acknowledgments, respectively. When mesh router A receives from B the acknowledgment for a before sent packet, A monitors the wireless channel until it hears the transmission of the same packet performed by B (towards C, see Figure 1(X)). If such transmission does not occur before the timer expires, A will accomplish that B has not forwarded its packet and will increment only the counter of the number of acknowledged packets.

To increase the opportunity to identify the forwarding behavior of nearby mesh routers, the monitoring node considers all the packets originated by nodes exclusive its transmission range. As shown in Figure 1(Y), A considers also the packets transmitted by D. If A does not hear the retransmission of the acknowledged packet sent by D before the timeout expires, it will conclude that B has dropped it; in this case, A will update only the number of packets acknowledged by A.

VI. CONCLUSION

It is aimed to select the most reliable path by considering both the quality of wireless links and the forwarding behavior of network nodes. To evaluate the effectiveness and the scalability of the proposed metrics through simulations. The results show that the Expected Forwarding Counter and two variants of solutions considerably increase both the network throughput and fairness with respect to the baseline approach that takes into account only the successful transmission rate of a wireless link. It can be concluded that the proposed metric and its refinements represent an effective solution for achieving highly resilient routing and thus high delivery rates in WMCNs.

ACKNOWLEDGMENT

We would like to thank our college Srinivasan Engineering College,PRINCIPAL Mr. K.Elangovan HOD Mrs. S. Jayanthi, our guide Mrs. S.Nandhini Devi, and other staff for their continuous support and for their helpful comments on the earlier drafts of this paper.

REFERENCES

[1] Aad, J.-P. Hubaux, and E. W. Knightly, “Impact of denial of service attacks on ad hoc networks,” Aug. 2008.

[2] L.Buttyan and J. P. Hubaux, “Enforcing service availability in mobile ad hoc WANs,” Jun. 2000.

[3] R.Draves, J.Padhye, and B.Zill, “Routing in multi-radio, multi-hoc wireless mesh networks,” Apr.2004.

[4] J. Eriksson, M. Faloutsos, S. V. Krishnamurthy, and C.MIT, “Routing amid colluding attackers,” 2007.

[5] W.Galuba, P.Papadimitratos, M.Poturalski, K.Aberer, Z.Despotovic and W.Kellerer, “Castor: Scalable secure routing for ad hoc networks,” 2009.

[6] Y. C. Hu, A.Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,”2005.

[7] S. Roy, D.Koutsonikolas, S. Das, and Y. C. Hu, “High-throughput multicast routing metrics in wireless mesh networks,” 2008.

[8] S.Stefano Paris, Cristina Nita- Rotaru, Fabio Matignon and Antonio “Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks”.

[9] Y. Wu, S. Tang, P. Xu, and X. Y. Li, “Dealing with selfishness and moral hazard in non-cooperative wireless networks,” Mar. 2009.