Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.253 – 262

RESEARCH ARTICLE

A WIRELESS MESH NETWORKS WITH RELIABLE AND RESILIENT ROUTING BY CROSS-LAYER METRICS

[1]M.Ranjith Priyanka, [2]J.Mary Metilda

[1]Department of Computer Science and Engineering, PG (M.E) Scholar, India

[2]Department of Computer Science and Engineering, Assistant Professor, India

[1] ranjithpriyankabe@gmail.com

[2] cse.metilda@gmail.com

ABSTRACT:

A Novel routing metric, Expected Forwarded Counter (EFW) to cope with a problem of selfish behavior (packet dropping) of mesh routers in a Wireless Mesh Networks (WMN).Wireless Mesh Networks emerged as a flexible and low cost network infrastructure, where heterogeneous mesh routers managed by different users collaborate to extend network coverage. EFW combines routing Layer observations of forwarding behavior with MAC Layer measurements of wireless link quality to select the most reliable and high performance path. The proposed metrics will be evaluated through both simulations and real-life deployments on two different wireless testbeds, performing a comparative analysis with On Demand Secure Byzantine Resilient Routing (ODSBR) Protocol and Expected Transmission Counter (ETX).Cross Layer metrics accurately capture the path reliability and Even when a high percentage of network nodes misbehave it increase the WMN performance.

Keywords-Routing metrics, Wireless Mesh Networks, Selfish behavior, wireless testbed

I. INTRODUCTION:

A Wireless Mesh Networks is defined as where each node is connected to many others, configured to allow connections to be rerouted around broken or blocked paths, from node to node until it reaches its destination. Link-Layer Metrics focused primarily on the detection of nodes that exhibit selfish behavior and on their exclusion from the network. Routing metrics that consider the selfish behavior of network nodes to increase the hop count of a network path proportionally to the number of selfish nodes that belong to that path. However, these metrics do not consider the wireless link quality, and thus fail to choose high-throughput paths between a source and a destination in the presence of selfish nodes that drop packets at the network layer.

A. PROBLEM DESCRIPTION:

Routing metrics proposed in recent 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 the above mentioned problem a cross-layer routing metric, EFW, and two alternative refinements, MEFW and JEFW, was proposed to select the most reliable path by considering both the quality of wireless links and the forwarding behavior of network nodes.
- A cross-layer metrics that selects the path with the highest packet delivery rate considering both the quality of wireless links and the reliability of network nodes. A new reliability metric (EFW) will be designed, 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. Two variants of EFW, 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 representation and the signaling overhead.

II. RELATED WORK:

In Wireless multihop networks with selfish participants has been proposed to address the problem based on detection and incentives techniques to enforce and obtain collaboration among network nodes.

A. DETECTION-BASED TECHNIQUES:

It comprise works like [7]-[10], which focus on detecting the dropping actions and, if needed, excluding the guilty nodes from the networks. Sprout is a routing protocol that probabilistically generates a multiplicity of link-disjoint paths to reach other network nodes and deliver the messages using the most reliable route.

B. INCENTIVE-BASED TECHNIQUES:

Defining the utility perceived by a network node as a function of the cost incurred in packet relaying and the reward obtained from the devices interested in the node collaboration. In [29], propose two forwarding approaches, the Packet Purse Model (PPM) and the Packet Trade Model (PTM), through which the intermediate modes trade in packets. Finally, observed that unlike path-based approaches can be integrated in several routing and forwarding schemes.

III. PROPOSED SYSTEM:

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.

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. EFW 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. MEFW and JEFW are the two variants of EFW which capture the worst and joint dropping behavior of the nodes that have established the wireless link.

Let (i, j) be the wireless link established between nodes i and j:p*ij* and p*ji* denote the packet loss probability of wireless link (i, j) in reverse and forward respectively.

$$EFW_{ij} = \frac{1}{p_{fwd,\,ij}} = \frac{1}{(1-p_{ij}).(1-p_{ji})} \cdot \frac{1}{(1-p_{d,\,ij})}$$

$$ETX = \frac{1}{p_{s,\,ij}} = \frac{1}{(1-p_{ij}).(1-p_{ji})}$$

Where $p_{fwd,\,ij} = p_{s,\,ij} . (1-p_{d,\,ij})$ the probability that a packet sent through a node *j* will be successfully forwarded can be computed,

The probability of a successful transmission on the wireless link *(i,j)* can be computed as $p_{s,\,ij} = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})}$.

A. SYSTEM MODEL:

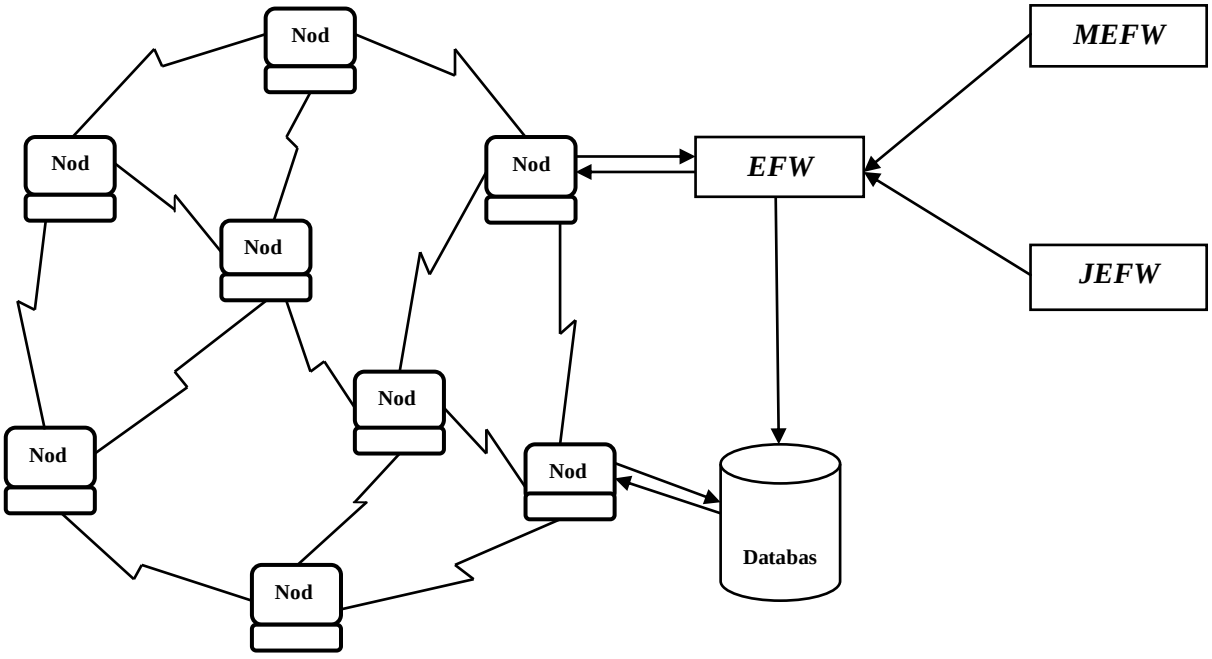

TABLE.1. DETECTION ERROR

One CBR Source (Fig. 1(a))				
CBR Traffic (Mb/s)	**0.1**	**0.5**	**1.0**	**1.5**
User	0%	1%	2%	5%
Kernel	0%	1%	3%	6%
Two CBR Sources (Fig. 1(b))				
CBR Traffic (Mb/s)	**0.1**	**0.5**	**1.0**	**1.5**
User	0%	2%	5%	10%
Kernel	0%	2%	2%	8%

Optimized Link State Routing Protocol (OLSR) are used by individual nodes to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

B. MINIMUM AND JOINT EXPECTED FORWARDING COUNTER METRICS (MEFW & JEFW):

MEFW, a close approximation of the EFW metric that considers only the worst dropping behavior. For each link(i,j) that a node i can establish with each neighbor j, we consider the maximum among the dropping probabilities of the two end nodes of the communication link, according to

$$MEFW_{ij} = MEFW_{ij} = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-\max\{p_{d,ij}, p_{d,ji}\})}$$

$$JEFW_{ij} = JEFW_{ji} = \frac{1}{(1-p_{ij}) \cdot (1-p_{ji})} \cdot \frac{1}{(1-p_{d,ij}) \cdot (1-p_{d,ji})}$$

IV. SIMULATION RESULTS:

The numerical results obtained evaluating the proposed routing metrics with the NS2 simulator [14].

A. EXPERIMENTAL METHODOLOGY

1. Nodes Configuration: As MAC and physical layers the implementation proposed in [44] since it models both layers more accurately than the basic version provided by NS2, including the cumulative signal-to-noise-pulse-

interference ratio (SINR)computation, the preamble and PLCP header processing, and a more realistic frame body capture.

2. Network Topologies: By comparing the proposed metrics(EFW, MEFW, and JEFW)to the standard ETX metric and the ODSBR protocol considering the two following network topologies.

- Grid Topology: The mesh routers from a square grid topology.
- Highly dense random topology: The nodes are randomly placed over the square area, forming a connected network. The minimum degree of all network nodes is fixed to 7.

3. Attack Scenarios: the two following scenarios

- No attack: There are no adversaries in the network. This scenario represents the ideal case and provides an upper bound on network performance for our scheme.
- Data dropping attack: In this scenario, the adversary nodes vary their packet drop rate in the 0%–100% range.

4. Adversary Nodes Placement: To provide a more complete comparison, we also evaluate two different placements of the adversary nodes. Specifically, we consider the following configurations.

- Anywhere placement: Any network node can be selected as selfish node.
- Central placement: Only nodes placed in the middle of the network topology can be selected to act selfishly.

5. Data Traffic Pattern: In the Grid topology, we establish seven data connections between each node in the first column and the corresponding destination node at the right end of the same row. In the Random topology, the source and destination nodes of the data connections are randomly selected among all network nodes. Evaluating the network performance using CBR and FTP traffic transmitted over UDP and TCP connections, respectively.

6. Performance Metrics: We consider as performance metrics the average packet delivery rate (PDR) achieved by the seven UDP connections and the network fairness measured using the Jain's Fairness Index.

The value of both metrics lies between 0 and 1. As for the Jain's Fairness Index, the higher the value, the greater the network fairness among the connections. Specifically, when the Jain's index is equal to 1, all connections experience the same throughput, whereas a value

equal to k/n indicates that only out of connections receive an equal share of the network bandwidth. Also evaluating the strength of the attacks described above on seven long-lived TCP connections using as metric the goodput decrease ratio (GDR), defined in [7] as

$$GDR = \frac{Zn - Za}{Zn}$$

Where Za and Zn represent the average goodput when the network is under attack and not under attack, respectively. Therefore, the higher the GDR is, the lower the resilience of the network against the attack.

B. Performance Analysis With Connectionless Traffic

- Effect of Adversary Size: First evaluating the effect of the number of adversary nodes on the network performance using the three proposed metrics, in terms of packet delivery rate and fairness of the established CBR connections. We vary the percentage of adversary nodes in the 10%–30% range. The mesh routers selected as adversaries drop all the traffic sent by other nodes.

In congested networks, installing a relatively high number of adversary nodes that drop less than 40% of the data traffic represents a better strategy for selfish community users than installing a low number of adversary nodes that drop all the data traffic. In the presence of adversary nodes with high dropping rates, the proposed metrics restore the network fairness, distributing the damage among all data connections, thus reducing the effectiveness of the attack.

C. Performance Analysis with Connection-Oriented Traffic

- Evaluating the effect of the dropping behavior on the performance of closed-loop, TCP connections. For the sake of brevity, we only show the performance achieved by the FTP connections varying the percentage of adversary nodes in the 0%–30% range.

Congestion control algorithms implemented by TCP reduce the opportunity to detect the forwarding behavior of intermediate nodes since they decrease the transmission rate when the connection experiences severe losses. To mitigate this problem, we can increase the validity time of the routes computed by OLSR.

V. CONCLUSION:

Routing metrics proposed in recent 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, a cross-layer routing metric, EFW and two alternative refinements, MEFW and JEFW, was implemented to select the most reliable path by considering both the quality of wireless links and the forwarding behavior of network nodes. The evaluation of effectiveness and scalability of the proposed metrics through simulations and real testbed measurements performed in typical network scenarios. That the proposed solutions considerably increase both the network throughput and fairness with respect to the baseline approaches that takes into account only the successful transmission rate of a wireless link. The proposed metric and its refinements represent an effective solution for achieving highly resilient routing and thus high delivery rates in WMNs.

REFERNCES

[1] S. Paris, C. Nita-Rotaru, F.Martignon, and A. Capone, "EFW: A crosslayer metric for reliable routing in wireless mesh networks with selfishparticipants," in Proc. IEEE INFOCOM, Apr. 2011, pp. 576–580.

[2] 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 Commun., vol. 14, no. 4, pp. 79–89, Aug. 2007.

[3] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A highthroughput pathmetric formulti-hop wireless routing," Wireless Netw.,vol. 11, no. 4, pp. 419–434, 2005.

[4] S. Roy, D. Koutsonikolas, S. Das, and Y. C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," Ad Hoc Netw.,vol. 6, no. 6, pp. 878–899, 2008.

[5] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," IEEE/ACM Trans. Netw., vol. 16, no. 4,pp. 791–802, Aug. 2008.

[6] I. Aad, J. P. Hubaux, and E.W. Knightly, "Denial of service resilience in ad hoc networks," in Proc. ACM MobiCom, 2004, pp. 202–215.

[7] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens,"ODSBR: An on-demand secure Byzantine resilient routing protocol
for wireless ad hoc networks," Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[8] W.Galuba, P. Papadimitratos,M. Poturalski,K. Aberer, Z.Despotovic, andW.Kellerer, "Castor: Scalable secure routing for ad hoc networks,"in Proc. IEEE INFOCOM, 2009, pp. 1–9.

[9] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 193–209, 2003

[10] J. Eriksson, M. Faloutsos, S. V. Krishnamurthy, and C.MIT, "Routing amid colluding attackers," in Proc. IEEE ICNP, 2007, pp. 184–193.

[11] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing inwirelessmesh networks," in Proc. IEEEGLOBECOM, 2008,pp. 1–5.

[12] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," RFC 3626, 2003 [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[13] "OLSRD: Ad hoc wirelessmesh routing daemon," [Online]. Available:http://www.olsr.org/

[14] S. McCanne, S. Floyd, and K. Fall, "Vint project U.C. Berkeley, ns-2 network simulator," [Online]. Available: http://www.isi.edu/nsnam/ns/

[15] B. Awerbuch, D. Holmer, H. Rubens, and R. Kleinberg, "Provably competitive adaptive routing," in Proc. IEEE INFOCOM, 2005, pp.
631–641.

[16] B. Carbunar, I. Ioannidis, and C. Nita-Rotaru, "JANUS: A framework for scalable and secure routing in hybrid wireless networks," IEEE
Trans. Depend. Secure Comput., vol. 6, no. 4, pp. 295–308, Oct.–Dec. 2008.

[17] W. Yu and K. J. R. Liu, "Attack-resistant cooperation stimulation in autonomous ad hoc networks," IEEE J. Sel. Areas Commun., vol. 23,
no. 12, pp. 2260–2271, Dec. 2005.

[18] X. Zhang, A. Jain, and A. Perrig, "Packet-dropping adversary identification for data plane security," in Proc. ACM CoNEXT, 2008, pp. 112.

[19] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," in Proc. IEEE INFOCOM, 2003,
vol. 2, pp. 808–817.

[20] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "An analytical approach to the study of cooperation in wireless ad hoc networks,"
IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 722–733, Mar. 2005.

[21] W. Yu and K. J. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," IEEE
Trans. Mobile Comput., vol. 6, no. 5, pp. 507–521, May 2007.

[22] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE INFOCOM,2003, pp. 1987–1997.

[23] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents,"in Proc. ACM MobiCom, 2003, pp. 245–259.

[24] S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 19–33, Jan.2008.

[25] J. J. Jaramillo and R. Srikant, "DARWIN: Distributed and adaptive reputation mechanism for wireless ad hoc networks," in Proc. ACM MobiCom, 2007, pp. 87–98.

[26] Y. Wu, S. Tang, P. Xu, and X. Y. Li, "Dealing with selfishness and moral hazard in non-cooperative wireless networks," IEEE Trans. MobileComput., vol. 9, no. 3, pp. 420–434, Mar. 2009.

[27] S. Zhong and F.Wu, "On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks," in Proc. ACM MobiCom,2007, pp. 278–289.

[28] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating participation inwireless community networks," in Proc. IEEE INFOCOM,Apr. 2006, pp. 1–13.

[29] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad hoc WANs," in Proc. ACM MobiCom, 2000, pp. 87–96.

[30] D. Johnson and G. Hancke, "Comparison of two routing metrics in OLSR on a grid based mesh network," Ad Hoc Netw., vol. 7, no. 2,pp. 374–387, 2009.

[31] G. Jakllari, S. Eidenbenz, N. Hengartner, S. V. Krishnamurthy, and M.Faloutsos, "Link positions matter: A noncommutative routing metric for wireless mesh network," in Proc. IEEE INFOCOM, 2008, pp.744–752.

[32] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in Proc. ACM MobiCom, 2004, pp. 114–128.

[33] S. Capkun, L. Buttyán, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan. 2003.

[34] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks,"Wireless Netw., vol. 11, no. 1–2, pp. 21–38, 2005.

[35] X. Ai, V. Srinivasan, and C. K. Tham, "Wi-Sh: A simple, robust credit based wi-fi community network," in Proc. IEEE INFOCOM, 2009, pp.1638–1646.

[36] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecturefor multihop wireless mesh networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[37] J. Eriksson, S. V. Krishnamurthy, andM. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. IEEE ICNP, 2006, pp. 75–84.

[38] M.E.M.Campista, P. M. Esposito, I.M.Moraes,L.H. M. Costa,O. C.M. Duarte, D. G. Passos, C. V. N. de Albuquerque, D. C.M. Saade, and M. G. Rubinstein, "Routing metrics and protocols for wireless mesh networks," IEEE Netw., vol. 22, no. 1, pp. 6–12, Jan.–Feb. 2008.

[39] K. H. Kim and K. G. Shin, "On accurate measurement of link quality in multi-hop wireless mesh networks," in Proc. ACM MobiCom, 2006,pp. 38–49.

[40] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp. 255–265.

[41] E. A. Tobagi and L. Kleinrock, "Packet switching in radio channels:Part II—The hidden terminal problem in carrier sense multiple access modes and the busy-tone solution," IEEE Trans. Commun., vol.COM-23, no. 12, pp. 1417–1433, Dec. 1975.

[42] J. Camp and E. Knightly, "The IEEE 802.11s extended service set mesh networking standard," IEEE Commun. Mag., vol. 46, no. 8, pp.120–126, Aug. 2008.

[43] Y. Yang and J. Wang, "Design guidelines for routing metrics in multihop wireless networks," in Proc. IEEE INFOCOM, 2008, pp.1615–1623.

[44] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi,and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in ns-2," in Proc. ACM MSWiM, 2007, pp. 159–168.

[45] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H.Kremo, R. Siracusa, H. Liu, and M. Singh, "Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols," in Proc. IEEE WCNC, 2005, vol. 3, pp. 1664–1669.

