ISSN 2348 – 9928
IJAICT Volume 2, Issue 10, October 2015 Doi:01.0401/ijaict.2014.03.18 Published Online 05 (10) 2015

CAPABILITY BASED ROUTING WITH SECURITY USING MOBILE AGENTS AND THREAT LOCATOR MECHANISM IN WIRELESS MESH NETWORK

Mr. Veershetty M Dagade
Lecturer,
Computer Science and Engineering,
Jain College of Engineering,
Belgaum, Karnataka, India

Dr. S. R. Mangalwede
Professor,
Computer Science and Engineering,
Gogte Institute of Technology,
Belgaum, Karnataka, India

Abstract— Wireless mesh networks (WMNs) pioneer a new type of network that has been applied over the last few years. Multicast routing is considered to be one of the most vital developing issue in WMN. which is a key technology that provides dissemination of data to a group of members in an efficient way. Despite recent advances in wireless mesh networking, various research challenges continue to remain in all protocol layers. Focusing on the network layer we propose our work on routing protocol. The interconnection of access points using wireless links exhibits great potential in addressing the issues like node capability in terms of processing power, memory, battery life etc. In this proposal, after an introduction about the structure of a WMN, some routing algorithms and protocols in WMNs are surveyed and a new routing algorithm CBR (Capability Based Routing) protocol is proposed with flow control, admission control, policy control, load balancing as part of routing process. Various admission control parameters with policy enforcement the packets can be made to transfer along a specified capable path with QoS commitment. So far many secure routing protocols have been proposed for ad-hoc networks, on the other hand, due to the different nature and characteristics they cannot perform well in a WMN environment. As part of our proposal we also discuss the limitations and challenges and propose an exclusive secure routing protocol that makes use of mobile agent for an infrastructure based wireless mesh network with threat locator mechanism. Our system is robust against a diversity of multi-hop threats and will perform well over a range of scenarios that would be tested.

Keywords - Wireless Mesh Network, Capability Based Routing, QoS, Security, Mobile Agents, Threat Locator Mechanism.

I INTRODUCTION

Wireless mesh networking has emerged as a promising design paradigm for next generation wireless networks. Wireless mesh networks (WMNs) consist of mesh clients and mesh routers, where the mesh routers/node as can be seen from the Fig 1 form a wireless infrastructure/backbone and interwork with the wired networks to provide multihop wireless Internet connectivity to the mesh clients. Wireless mesh network has one of the most promising concepts for self-organizing and auto-configurable wireless networking to provide adaptive and flexible wireless Internet connectivity to mobile users. WMN is formed automatically once the mesh nodes have been configured and activated, which reduces setup time and maintenance cost, owing to its self-forming nature. This idea can be used for diverse wireless access technologies such as IEEE 802.11, 802.15, 802.16-based wireless local area network (WLAN), wireless personal area network (WPAN), and wireless metropolitan area network (WMAN) technologies, respectively. Potential application scenarios for wireless mesh networks include backhaul support for cellular and home networks, enterprise networks, community/society networks, and intelligent transport system networks [1, 2].

Development of wireless mesh networking technology has to deal with challenging architecture and protocol design issues, and the researchers in both academia and industry have shown interest on this technology. There are many on-going research projects in diverse universities and industries/engineering research labs. Also, lots of startup companies as well as established industries are building mesh networking platforms based on off-the-shelf wireless access technologies and developing demanding applications and services.

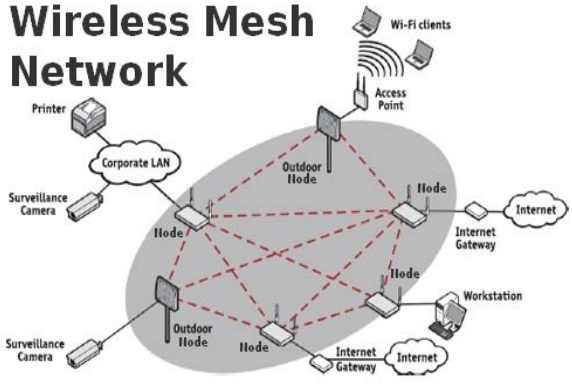

Fig 1 : Wireless Mesh Network

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers are not mobile and form the backbone of WMNs. They provide network service access for mesh and clients attached. The gateway and bridging functions in the mesh routers help integrate WMN with networks like internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc. Mesh clients are most of the times mobile devices however they can be stationary, and can form a client mesh network among themselves and with mesh routers. WMNs are likely to resolve the limitations and to significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs). They are undergoing rapid progress and inspiring numerous deployments. Wireless services are transported by WMN for a large diversity [3] of applications in personal, local, metropolitan areas and including campus. In spite of fresh advances in wireless mesh networking, numerous research challenges stay in all protocol layers. Hence based on detailed study on recent advances and open research issues related to routing in WMNs we propose a CBR based routing protocol. We need to understand that WMN is not comprised of only stationary electricity/generator driven routers but it also comprises of devices like PC, desktop computers, Laptops, Mobile phones, Tablets, PDA's etc which are well equipped with the needed NIC card for getting and giving the service from and to the WMN. We also need to understand the capabilities of the devices connected to WMN that is our focus of discussion in our proposal [4].

If we consider capabilities of a device, many factors like processing power of the device, memory capacity of the device, battery life etc come into picture. People using WMN service may be dealing with variety of applications in the form of Audio, video, text, images etc where QoS commitment needs to be taken care of. Suppose a user wants to transfer a video file on WMN, we know that in WMN any device connected can act as router forwarding packets so a question arises about the intermediate devices capability to forward the video packets and in a given rate and QoS commitment. Considering the above case we are proposing a model **CBR** (Capability based routing) where, in the router some configuration is done to classify the incoming packets into text, audio, video etc and schedule the individual classified packets at a given rate. Proper Admission control and Policy Control modules are needed in order to provide QoS commitment. As part of our proposal we are also concerned about the security of the packets being transferred. However, wireless medium and multihop communication let the action of attackers that can violate data packets or compromise the routing service, plummeting performance and QoS (Quality of Service) of applications [5]. Even in ordinary conditions of the network, without the presence of attackers, interferences in the shared wireless medium lessen the overall performance of paths. Such aspects require the development of new routing administration approaches to address security and performance together [6].

We propose a novel strategy by employing mobile agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as wandering agents that tour the network and decoy attackers by sending route request advertisements. We collect important information on attacker's tactic from the intrusion logs gathered at a given threat Locator mechanism. We finally evaluate the effectiveness of the proposed architecture using simulation in NS-2. The same can be achieved practically if WMN compatible devices are available [7].

II LITERATURE SURVEY

Different solutions have been designed to attain performance goals on routing in wireless multihop networks. CORMAN [10] is an opportunistic routing scheme to enhance throughput on mobile ad hoc networks. In this scheme, different packets of the same flow can take different paths to a destination based on the transient link quality of wireless channels.

Yang et al. [11] proposed a geographic routing protocol to provide reliable data delivery on high mobile wireless networks. In that protocol, when a source node sends a data packet, neighbor nodes that overhearing the transmission are considered as forwarding candidates, and forward the packet, if it is not relayed by the specific best forwarder within a certain time slot than an alternate forwarder is chosen.

Cheng et al. [12] proposed a robust forwarding extension (RFE) for on demand routing protocols in wireless ad hoc networks with unreliable links. RFE aims to mitigate the wireless channel variation effects using the local path diversity in the link layer. It also applies the basic greedy forwarding rule in geographic routing, i.e., data packets are forwarded to all neighbors geographically closest to the destination.

A hybrid on demand distance vector routing (HOVER) algorithm for wireless mesh network is proposed in [13],

which is again based on AODV. It is node aware routing having the capability of link quality estimation and optimal link selection.

A resilient and opportunistic mesh routing (ROMER) [14] balances both the long term route stability and short term opportunistic performance to overcome the problem of unstable links by delivering redundant data copies. SrcRR [15] is another routing protocol for WMNs, which focuses to achieve high throughput. HEAT [16] is a scalable routing protocol in wireless mesh networks use temperature fields. Every node has a temperature value, and the packets are routed towards the gateway on the basis of increasing temperature values.

Examples of QoS multicast routing protocol in wireless multi-hop networks include Lantern-trees [17], QAMNet [18], OMRPCAH, and ODQMN [19, 20]. QoS multicast schemes aim at identifying a set of required components: QoS routing, resource reservation, and QoS capable MAC layer [21]. QoS schemes need to identify potential segments (links and routers) in the network that may have sufficient resources to meet the required QoS routing.

Huang et al. [8] proposed a cooperative Intrusion Detection System (IDS) in an ad hoc network for various kinds of attacks. The authors assume that an attacker may not only try to affect the routing protocol in the ad hoc network but also the IDS. The authors perform an anomaly detection technique using correlation, assuming that there exists a strong correlation if they are normally behaving.

But this is not the same when malicious behavior is present. Hence, they use such correlation to detect the abnormal behavior. However, with the anomaly detection system, the results obtained for a blackhole attack are less effective. The authors also identify the attack type where they use a "monitoring" node and a "monitored" node, where the function of the monitoring node is to analyze the behavior of the monitored node [9].

Islam et al. [9] proposed a Secure Hybrid Wireless Mesh Protocol (SHWMP) which uses cryptographic extensions to ensure authenticity and integrity on HWMP routing messages and prevents unauthorized manipulation of mutable fields in routing information elements. However, SHWMP is vulnerable to the attacks launched by internal legitimate mesh routers due to two reasons. First, it assumes that all internal mesh routers cooperate with each other without interrupting the operation of protocol. Second, SHWMP uses a hop-by-hop authentication mechanism to provide security of routing messages: each mesh router decrypts received packets and re-encrypts them using its own key. In this way, user privacy information is partly protected from eavesdroppers but not mesh routers because of routing in the mesh backbone. Thus, an active attacker can compromise and control mesh routers to obtain user privacy information.

Samad et al. [21] proposed a protected neighborhood-based trust mechanism in clustered wireless mesh networks. The mechanism is based on neighborhood trust to gain required security and identification privacy in a clustered WMN. However, some privacy information of users has to be disclosed to the relay mesh routers, which makes malicious mesh routers be able to get the privacy information.

Khan et al. [22] proposed SRPM, an improvement of AODV for an infrastructure based wireless mesh network. In SRPM, to ensure security, it keeps the information of two-hop neighbors unlike to AODV, which keeps one-hop information in the routing table. To further increase the security level, it introduces a new routing metric, which is capable of searching the shortest secure path by computing Unreliability Value (UV) of the neighbors. However, the SRPM is vulnerable to the attacks launched by internal legitimate mesh routers and cannot provide privacy protection effectively.

Ren et al. [13] proposed PEACE, a novel privacy-enhanced yet accountable security framework, tailored forWMNs. PEACE is presented as a suite of authentication and key agreement protocols built upon short group signature variation. However, PEACE only secures the network from external attacks and takes it for granted that every internal node is cooperative and trustworthy

This paper addresses the routing issues in a WMN, by considering the specific characteristics of a WMN. It explores open solutions, and evaluates their appropriateness to the wireless mesh environment.

Based on this assessment, the need for developing new routing mechanisms, specifically tailored for the unique characteristics of WMNs is assessed. In order to guide future work and development of a WMN routing protocol, a number of issues and considerations are identified and presented.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.03.18 Published Online 05 (10) 2015

III OBJECTIVES

The main objective of our work is to design a new routing protocol CBR (Capability Based Routing) which takes care of most of the parameters of QoS like

- Packet classification
- Congestion Control
- Flow Control
- Policy Control
- Admission Control
- Load Balancing
- Differentiated services
- Best effort services

Another objective is to provide a security module using agent technology which helps in detecting threats like "Black Hole" attack and to take counter measures for such attacks making our proposal secure too.

IV METHODOLOGY

The Fig 2 depicts our proposed model CBR. As you can observe from the Figure that there are various modules as part of the proposed design, each module has certain functionality to be performed. The overall operation of our proposal can be understood with respect to the Fig 2 by the below steps.

1. In the first step as can observe from the figure all the incoming packets at the router are classified and placed in separate queue. This is packet classification process.

2. Next based on the type of packet various flow rates are assigned by the Rate Allocation module and next the scheduler contacts the Admission Control module to do a survey on resources allocation for the individual packets to forward.

3. Upon receiving the request by the scheduler the Admission Control module creates an agent to do a survey about the neighboring nodes about their capabilities with respect to processing power, memory [buffer], battery life etc.

4. Based on the information collected by the agent the admission control module next contacts the CBR module to make a decision to forward the packets on a reliable path.

5. The CBR module is one of the intelligent module which maintains a log of all the possible paths, so the module blindly does not forward the packets to the best path comprising of the intermediate nodes that are capable of forwarding the specific packets, but instead it contacts the Security module to get security related information about the path specified by the admission control agent.

6. Next the security module upon the request received to find the integrity of a path the module creates an agent to do a survey along the mentioned path to check whether the path is secure or not. The agent mainly checks for "Black hole" attack made by the intermediate node.

7. Upon gathering the information of the mobile agent the security module intimates the CBR module about the status of the path that the CBR module requested for. If the path is secured then the CBR module forwards the packets along the path, but if the path is not secured the CBR module does not forward the packets along the path rather the module checks for the next best path from the log file maintained.

8. Lastly the routing table is updated based on the secure status of the path

Note: All the modules are part of routing process as can be seen from the figure, that all the modules are controlled and coordinated by the routing process module [Routing]

In this proposal, we specifically focus on the problem of detecting malicious MRs (Malicious Routers) that bypass route lookup process and instead broadcast spurious route replies to all incoming route request query. Route replie is generated in such a way that any source is encouraged to choose this MR as an intermediate MR to route its traffic. It falsifies the sequence number field (high) and the hop count (low) field in the reply packet and advertises itself as the best possible route.

A sequence number field in a routing protocol reflects the freshness of the route and the hop count reflects the distance between the replying MR and the destination MR under question. In essence, it traps all the MRs in its neighborhood and lures them to route their traffic towards itself. Upon receiving the data traffic, it unscrupulously drops all the

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.03.18 Published Online 05 (10) 2015

traffic. Thus, in a way the malicious MR imitates the "blackhole" in the Universe that attracts all particles towards itself due to its enormous gravitational pull. Hence, we synonymously name this egregious MR as a "blackhole node" or "blackhole MR" in the network and the attack is called a "blackhole attack" [4].

Thus, Blackhole attack is a severe attack that exploits the hidden vulnerabilities in the routing protocol of wireless networks. The only possible counter-measure to prevent infiltration of such an attack is to authenticate the sequence number and hop count updates received from other nodes. Though secure routing protocols such as SEAD [5], Ariadne [6] attempt to address this issue, it is not a complete solution to thwart such an attack as MRs is deployed at public places. Here, we propose a pervasive monitoring that pro-actively supervises the routing process and ensures healthy operation.

4.1 Security module

As can be seen from the Fig 3 in the security module which is the magnified version of the security module available in the proposed model. The module creates an agent the agent generates a Route Request (RREQ) to a destination to which it already knows the route. This is called dummy RREQ because the agent does not originate any data traffic.
Instead, it generates such a request for the sole purpose of luring blackhole nodes to send a falsifieds reply. Unlike traditional honeypots, which capture only packets directed to them, our proposed mobile mechanism is very attractive to lure all attackers in the network. Upon seeing the RREQ of the agent, a malicious blackhole node produces a falsified route reply (RREP). It advertises itself as the best path (high sequence number and shortest hop) to a given destination.

The agent, in turn, generates a dummy data packet to be sent to a randomly chosen known destination. It is termed as a "known destination" because the agent is aware of an alternate route to that destination MR. Then the agent queries the destination through the known route that it is already aware of, to determine the integrity of the malicious node. Thus, we exploit the availability of multipath routing option available in WMNs [17] to validate the integrity of a route reply originating from node.

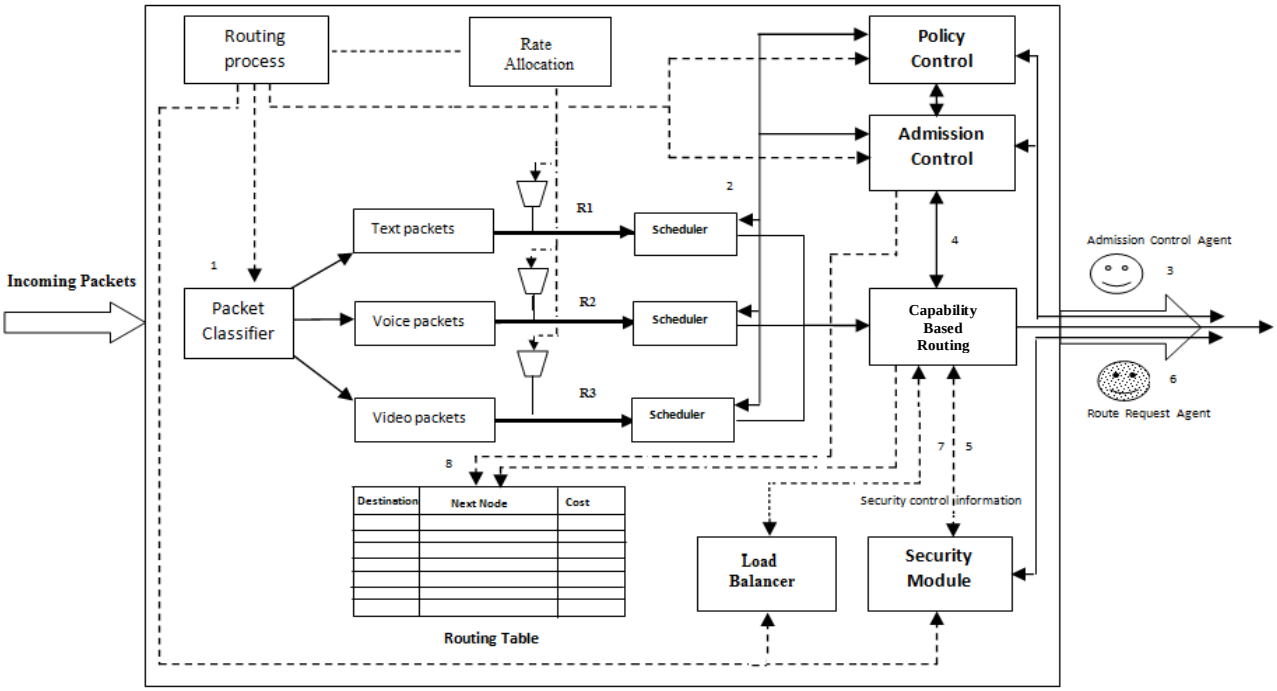

Fig 2 : Capability Based Routing

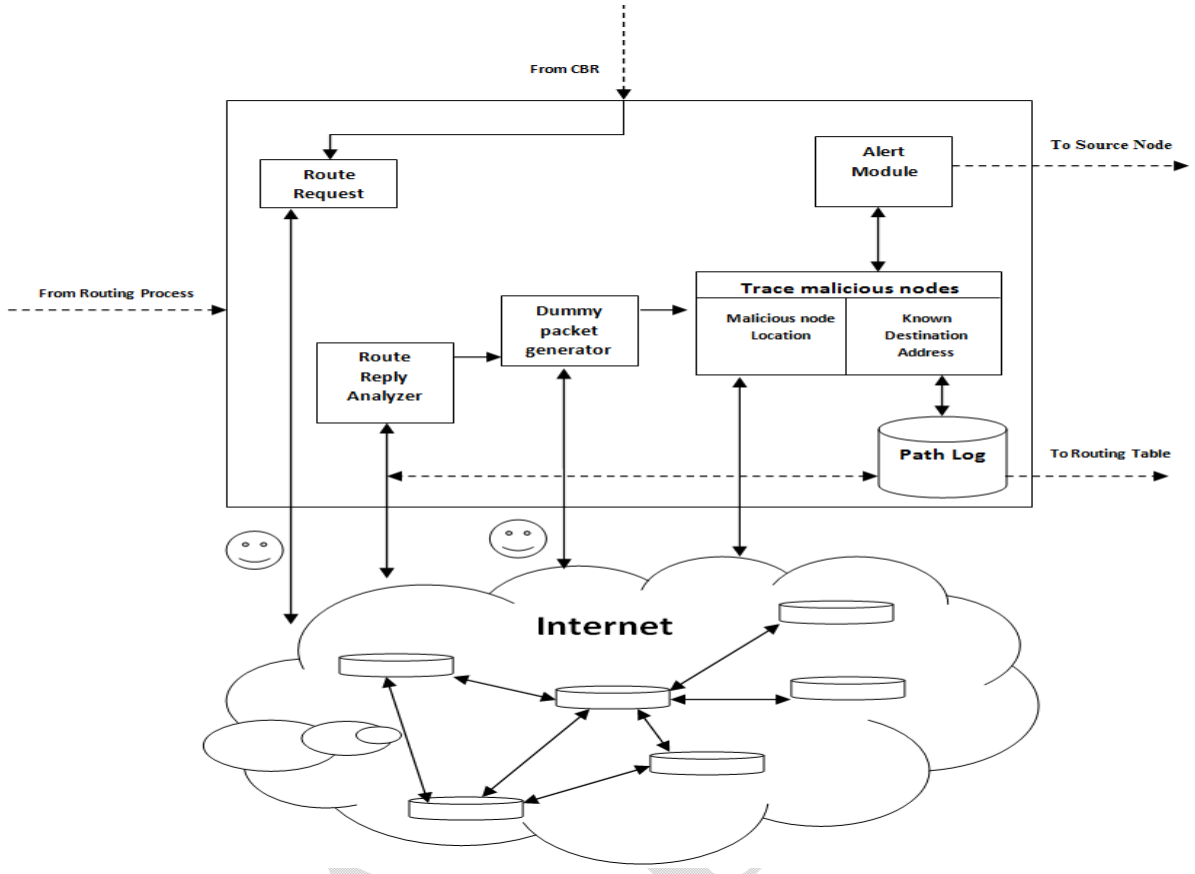

Fig 3 : Security Module

4.2 Outcomes

The outcomes of the proposed system is a new routing protocol CBR (Capability Based Routing) that takes care of most of the QoS Commitment. The research modules with respect to WMN have following outcomes

- ***Packet Classifier:*** This module helps in classifying the type of packets and provide certain different services to the individual packets
- ***Admission Control:*** This module helps to compute the resources (typically bandwidth, memory for buffer, processing power, battery life etc) requirements of new flow and determines whether the resources along the path to be followed by the flow are available
- ***Policy Control:*** This module helps in preventing the source from violating its contract, the network may want to monitor the traffic flow continuously hence this module serves the purpose
- ***Flow Control/Traffic shaper:*** This module helps in altering the traffic flow as per the QoS Commitment
- ***Congestion Control:*** This module helps avoiding dropping of packets by providing a buffer or queue
- ***Security:*** This module helps in secure routing and forwarding of packets
- ***Load balancer:*** For better management of available resources good load balancing techniques are required. So that loads balancing in WMN becoming more interested area of research. Load balancer improve both resource utilization and job response time while also avoiding a situation where some of the nodes are heavily loaded while other nodes are idle or doing very little work.

V CONCLUSION

After discussing about the objectives of our proposed system and seeing the outcomes we can say that our proposed system can serve as an alternative for routing packets in a secured manner with most of the parameters of QoS being met. Here we propose an intelligent agent based system to detect black hole

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.03.18 Published Online 05 (10) 2015

attackers in WMNs for the considered topologies. We model the detection mechanism of malicious black hole attackers using a detection agent with threat locator. The black hole attack severely affects the performance and other criteria of the WMNs and the agent based detection system raises a timely alert of an attack occurrence. Through extensive simulations, we demonstrate that our agent based detection model has a high detection rate and a low false positive rate. As a part of our future work, we plan to use threat locator agents to detect other types of attacks. We also plan to use the WCETT (Weighted Cumulative End-To-End Delay) as a routing technique to detect the blackhole attackers in the WMNs.

References

[1] Mohsen Jahanshahi, Alireza Talebi Barmi "Multicast routing protocols in wireless mesh networks: a survey" Computing DOI 10.1007/s00607-014-0403-z, © Springer-Verlag Wien (2014)

[2] Amr Alasaad, Hasen Nicanfar, Sathish Gopalakrishnan, Victor C. M. Leung, "A ring-based multicast routing topology with QoS support in wireless mesh networks" Wireless Netw (2013) 19:1627–1651 DOI 10.1007/s11276-013-0559-z, Springer Science+Business Media New York (2013)

[3] Anoosha Prathapani, Lakshmi Santhanam, Dharma P. Agrawal, "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents" J Supercomput (2013) 64:777–804 DOI 10.1007/s11227-010-0547-3 © Springer Science+Business Media, LLC (2011)

[4] Hu Y, Johnson DB, Perrig A "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks". Ad Hoc Netw 175–192 (2003).

[5] Khattab S, Melhem R, Mosse D, Znati T "Honeypot back-propagation for mitigating spoofing distributed Denial-of-service attacks". J Parallel Distrib Comput 66:1152–1164 (2006).

[6] Vinod Kone, Sudipto Das, BenY.Zhao, Haitao Zheng, "QUORUM—Quality of Service inWireless Mesh Networks" Mobile Netw Appl (2007) 12:358–369 DOI 10.1007/s11036-008-0050-8, © Springer Science + Business Media, LLC (2008)

[7] Yajun Li, Yunfeng Xiong, Liang Zhou, Rongbo Zhu, "Adaptive Optimization-based Routing in Wireless Mesh Networks" Wireless Pers Commun 56:403–415, DOI 10.1007/s11277-010-9979-6, © Springer Science+Business Media, LLC. (2011)

[8] Huang B, He Y, Perkins D, "Investigating deployment strategies for multi-radio multi-channel residential wireless mesh networks", IEEE Comput Soc 147–153 (2009)

[9] Wang, Z., Chen, Y., Li, C. "CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks". IEEE J. Sel.Areas Commun. 30(2), 289–296 (2012).

[10] Yang, S., Yeo, C.K., Lee, B.S. "Toward reliable data delivery for highly dynamic mobile ad hoc networks". IEEE Trans. Mob. Comput. 1(1), 111–124 (2012).

[11] Cheng, L., Das, S., Chen, C., Ma, J., Wang, W. "Robust forwarding for reactive routing protocols in wireless ad hoc networks with unreliable links". In: IEEE International Conference on Communications, pp. 1–6 (2011).

[12] Mir, S., Pirzada, A.A., Portmann, M. "HOVER: hybrid on-demand distance vector routing for wireless mesh networks". Proceedings of 31st Australasian Science Conference (ACSC) (2008).

[13] Tebbe, H., & Kassler, A. "QAMNet: Providing quality of service to ad-hoc multicast enabled networks". In Proceedings of the 1st intenational symposium on wireless pervasive computing (pp. 1–5). doi:10.1109/ISWPC.2006.1613664 (2006).

[14] Layuan, L., & Chunlina, L.. "A QoS multicast routing protocol for clustering mobile ad hoc networks". Computer Communications, 30(7), 1641–1654 (2007).

[15] Ng, J., Low, C. P., & Teo, H. S. "On-demand QoS multicast routing and reservation protocol for MANETs". In Proceedings of the IEEE PIMRC (pp. 2504–2508) (2004).

[16] Xiang, X.,Wang, X., & Yang, Y. "Supporting Efficient and scalable multicasting over mobile ad hoc networks". IEEE Transactions on Mobile Computing, 10(5), 544–559 (2011).

[17] Acharya, P. A. K., & Belding, E. M. MARS "Link-layer rate selection for multicast transmissions in wireless mesh networks", Ad Hoc Networks, 9(1), 48–60 (2011).

[18] Kumar N, Chilamkurti N, Lee JH "A novel minimum delay maximum flow multicast algorithm to construct a multicast tree in wireless mesh networks", Comput Math Appl 63(2) (2012).

[19] Zouaoui EME, Derdouri L, Zeghib N "Dynamic multicast membership algorithms for multichannel multi-radio wireless mesh network", Int J Comput Sci Telecommun 3(12) (2012)

[20] Avesh K. Agarwal, WenyeWang, "An Experimental Study of the Performance Impact of Path-Based DoS Attacks inWireless Mesh Networks" Mobile Netw Appl (2010) 15:693–709 DOI 10.1007/s11036-009-0204-3, © Springer Science + Business Media, LLC (2009)

[21] Helber Silva, Aldri Santos, Michele Nogueira "Routing management for performance and security tradeoff in wireless mesh networks" Int. J. Inf. Secur. DOI 10.1007/s10207-014-0246-9 © Springer-Verlag Berlin Heidelberg (2014)

[22] Huang Y-A, Lee W "A cooperative intrusion detection system for ad hoc networks", In: Proceedings of 1st ACM workshop on ad hoc and sensor networks, pp 135–147 (2003).