Cross Layer based Secured Route Optimization Technique for Wireless Mesh Networks-A Research Proposal

Parutagouda S Khanagoudar
Asst.Professor, Dept of CSE
KLS Gogte Institute of Technology
Belagavi. Karnataka state,India

Dr.G.M.Patil
Dept. of Electronics & Instrumentation Engineering,
Dayananda Sagar College of Engineering
Kumarswamy Layout
BENGALURU - 560 078
(Karnataka State), India.

Abstract:Wireless mesh network is made up of wireless radio nodes. Nodes/links in wireless Mesh Network may go down or even they may fail due to various reasons such as a) Dynamic bandwidth demands by various applications in the network b) Physical obstacles in the network c) co-channel interference and d) Attacks against routing. The main objective of the research proposal is to increase overall performance of the network and avoid manual configuration of network involved in maintenance of WMN and also developing an application runs on every network device and continues monitoring is carried to identify failure in node/link failures in WMN. ns2-based simulation is used to get the results.

Keywords: WMN, CO-CHANNEL INTERFERENCE, CROSS-LAYER DESIGN, PACKET DELIVERY RATIO, PACKET LOSS RATIO

I. INTRODUCTION

1.1 Wireless Mesh Networks

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. **[1]** Wireless mesh networks (WMNs) offers low-cost high-bandwidth community wireless services.**[2]**

The architecture of WMNs can be classified into three types: **[3]**

- *Infrastructure/Backbone WMN*

In this architecture, mesh routers form an infrastructure for clients. The mesh routers form a mesh of self-configuring, self-healing links among themselves.

- *Client WMN*

Client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing.

- *Hybrid WMN*

This architecture is the combination of infrastructure and client meshing.

1.2 Characteristics of WMNs

The characteristics of WMNs are outlined below, **[3]**

- WMNs support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization.

- WMNs are multi-hop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers.

- Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.

1.3 Applications of WMNs

Numerous applications envisioned to be deployed in WMNs, **[1]** such as web cast, 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.

1.4 Security Issues in WMNs

Security is the vital problem in WMNs. Battery, mobility and bandwidth constraints of WMNs pose challenges in achieving security goals. Some of the security issues are described below, **[4]**

- *Signal Jamming*

On the physical and media access control layers, an attacker can attack on availability of the network by employing jamming to interface with communication on physical channel.

- *Denial of Service (DoS)*

A DoS attack can be launched at any layer of wireless mesh network. There are many ways of instigating DoS. A common technique is to flood the target system with requests. The target system becomes so overwhelmed by the request that it could not process normal traffic**. [4]**

- *Tempering*

Routing protocols in WMN does not check the integrity of the packet. This allows the attacker could easily temper any specific field in the packet resulted in wrong routing decisions like re-direction or route loops, which degrades the performance of the entire network.. **[5]**

- *Wormhole attack*

Two distant points in the network are connected by a malicious connection using a direct low-latency link called the wormhole link. Once the wormhole link is established, the attacker captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

- *Black hole Attack*

While receiving routing request, the attacker claims that it has a link to the destination node even if it does not and then force the source to send packet through it without forwarding the data packet to next hop. **[5]**

1.5 Routing in WMNs

Whenever a node has to send some data to another node, it checks if it has the route to destination; if not it starts the route discovery phase. **[6]**Routing protocols are used to find and maintain routes between source and destination nodes, in order to forward traffic. Mesh routers are relatively static and Mesh routers are not power constrained. **[7]**

1.6 Issues of Security in Routing

Some of the issues are described below,

- By attacking the routing mechanism, an adversary can modify the network topology and therefore affect the good functioning of the network. **[8]** The adversary can,
  - Tamper with the routing messages,
  - Modify the state of one or several TAPs in the network,
  - Use replicated node(s),
  - Perform DoS attacks.
- *Transmission errors*
  The unreliability of the wireless medium may lead to transmission errors. **[7]**
- *Link and node failures*
  Nodes and links may fail at any time due to different types of hazardous conditions in the environment.
- *Incorrect routes*
  Due to node/link failures or additions to the network, routes may become obsolete or based on an incorrect system state. **[7]**
- *Congested nodes or links*

Due to the topology of the network and the nature of the routing protocols, certain nodes or links may become congested, which will lead to higher delay or packet loss.

II. RELATED WORK

Muhammad Shoaib Siddiqui [6] have proposed a security management mechanism for multi-path routing which efficiently uses the characteristics of WMNs, mutual authentication and secrete key cryptography to provide secure multi-path route management.

Md. Shariful Islam et al. [9] have proposed a secure version of HWMP (SHWMP) that operates similarly to that of HWMP but uses cryptographic extensions to provide authenticity and integrity of routing messages and prevents unauthorized manipulation of mutable fields in the routing information elements.

Zonghua Zhang et al. [10] have proposed a reputation-based anomaly detection scheme, called RADAR. Reputation is used to evaluate each node. A secure and dependable reputation management mechanism is used to propagate the trust values of each node. This mechanism ensures robustness and accuracy.

Wei Wang et al. [11] have proposed a joint routing scheduling scheme that achieves robust performance under traffic information uncertainty. It does not require accurate traffic information. Specifically, it only needs a rough estimation of the traffic demand. Therefore, this scheme is feasible and has affordable overhead.

Byung Joon Oh and Chang Wen chen [12] have proposed a novel cross-layer framework for MAC Protocol for a QoS-guaranteed delivery of the H.264 video streaming over wireless mesh networks. Based on the unique feature of wireless mesh networks, they have developed a Cross-Layer Adaptation HCCA MAC making full use of the Link Capacity Estimation Information for the adaptation as well as the application of video-Adaptive FEc to combat wireless channel impairments. They have also adopted both network level QoS metrics. Results shows that this scheme is able to substantially outperform the state-of-the-art scheme PRBACHCCAMAC with an average of 5.5dB in reconstructed video quality. However it is not scalable and can't support robust time-bounded media applications.

Yuhuai Peng et al.[13] have proposed a Cross-Layer QoS aware routing protocol based on OLSR(CLQ-OLSR) to support real-time multimedia communication by efficiently exploiting multiradio and multi-channel methods. By constructing multi-layer virtual logical mapping over physical topology, they have designed two sets of routing mechanisms. Physical modified OLSR protocol (MOLSR) and logical routing to accommodate network traffic. By piggybacking bandwidth information in HELLO and Topology Control(TC) messages, each node disseminates topology and bandwidth information in the whole network.

Narayan D G et al.[14] have proposed a joint problem of routing and interface assignment for Multi-Radio Wireless Mesh Networks to improve the performance of the network. They have designed a novel cross layer routine metric called Interference and Congestion Aware metric by considering Re-transmission count(RTC) from MAC layer,congestion at different interfaces of each node and intra-flow interference to find the optimal path. The results reveal that this joint approach performs better in terms of throughput,average end-to-end delay and packet delivery fraction. However video packets have more throughputs compared to audio and data packets which are least. This is because video packets are queued in lightly loaded interface, audio packets in medium loaded interface and data packets in highly loaded interface.

Hongfeng wang Dingding Zhou Shi Dong [15] have proposed a cross-layer opportunistic routing algorithm for ad hoc networks is proposed, which is called the multi channel(MCPEF) algorithm. Through local control actions,MCPEF aims to maximize the network throughput.MCPEF is shown through numerical model-based evaluation and discrete-event packet-level simulations to outperform baseline solutions. The estimation of residual bandwidth using the accuracy still needs to be improved.

Table 1 Summary of Significant Techniques/Mechanism evolved in recent years

Sl.no	Author	Technique /Mechanism Applied	Drawbacks
1	***Muhammad Shoaib Siddiqui* [6]**	Mutual authentication and secrete key cryptography	Does not provide 100% accuracy.
2	***Md. Shariful Islam et al.* [9]**	Uses cryptographic extensions	Fails in identifying the black hole attack ,increases network overhead
3	***Zonghua Zhang et al.* [10]**	Reputation-based anomaly detection scheme	Does not support for optimized routing
4	***Wei Wang et al.* [11]**	Robust routing and scheduling mechanism	No guarantee in finding shortest path
5	**Byung Joon Oh and Chang Wen chen [12]**	Novel Cross-layer framework for MAC Protocol	Not scalable and can't support robust time-bounded media applications.
6	**Yuhuai Peng et al.[13**	Cross-Layer QoS aware routing protocol based on OLSR(CLQ-OLSR)	Less control of the wormhole attack
7	**Narayan D G et al.[14]**	Joint problem of routing and interface assignment for Multi-Radio Wireless Mesh Networks	Minimum throughput for audio and data packets
8	**Hongfeng wang Dingding Zhou Shi Dong [15]**	Cross-layer opportunistic routing algorithm for ad hoc networks	Estimation of residual bandwidth using the accuracy still needs to be improved.

III. PROBLEM IDENTIFICATION

In general, the most challenging issue in wireless mesh network is secure routing. In WMNs, the backbone routers and wireless clients form unique two-tier architecture, with distinct mobility and power constraints. Backbone routers communicate via multi-hop wireless links, which have high loss rate and latency. **[2]**

Designing an efficient secure routing in wireless mesh network is difficult due to WMN constraints such as computation power, mobility of nodes and limited bandwidth.

In **[11]**, the authors have proposed robust routing and scheduling mechanism for wireless mesh networks. It works under dynamic traffic conditions. This mechanism can not guarantee the shortest path because it does not consider hop count metric as a major metric. Also, it does not work well when other factors dominate. Instead of providing secure routing mechanism it serves as traffic controlling mechanism.

A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network is proposed in **[9]**
To provide secure routing, this protocol adds MAC value with the routing messages which eventually increase overhead.

CSROR **[16]** selects an optimum route on the basis of routing security, taking in consideration the different cross layer parameters. Though CSROR is resource aware, but it is resilient only to packet dropping attacks.

IV. RESEARCH OBJECTIVES

The primary goal of this proposal is to develop a new secured routing protocol for WMN with the following objectives:

- To determine Resource efficient shortest path and defend black hole attack against routing.

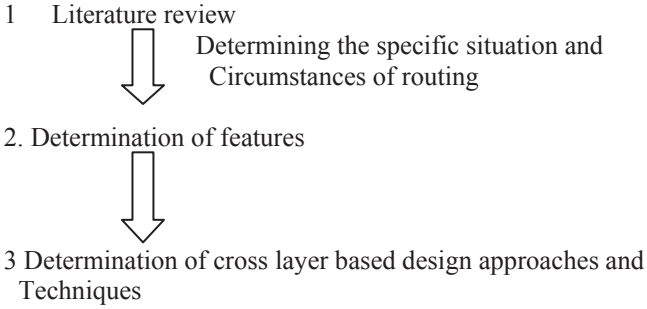
- To improve the quality of service in WMN by reducing the number of hops and communication overhead generated in the network.

- To determine maximize network throughput by performing joint routing, scheduling and transmit power control.

V. RESEARCH METHODOLOGY

The research scope lies in the Network Simulator (NS2). The NS2 is an open source programming language. NS2 is a discrete event time driven simulator which is used to mainly model the network protocols.
Our methodology is based on

- Determination of scope based on extensive literature
- The features are identified using digital communication and networking concepts based on our specific objectives.
- Designing of protocol is based on experiments and method 1 and 2.



The research work is split into two steps as follows.

Steps 1:

- Creation of Network Topology:
  i) Mesh topology is created with the number of nodes, routers and gateway in the network.
  ii) Select the source and destination for the transmission of data.

Steps 2:

- Transmission of data from source to destination:
  i) By considering the static architecture with 10 nodes,2 routers and 1 gateway in the beginning, by limiting this static structure use the onion routing algorithm for transmission of data by using some encryption techniques to see that quality of service and security is maintained in routing from the source to the destination. Record the performance in terms of simulation graph .By this objective 1 can be achieved.
  ii) Changing the source and destination, number of nodes and routers each time and evaluate the performance by varying the simulation time, transmission range. Apply the angle based routing and record its performance. By this objective 2 can be achieved
  iii) By considering the parameters like packet delivery ratio, packet loss ratio, delay etc and joint routing, objective 3 can be achieved.

EXPECTED OUTCOMES

- Identification and determination of routing features to determine resource efficient shortest path—supported by experimental results.
- Determination of best and optimal routing protocol supported by experimental results with comparisons.
- Determination of specific situation and context for determining the secured routing.
- A better framework will be implemented based on cross layer based design.

REFERENCES

[1] Jing Dong, Reza Curtmola and Cristina Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks", IEEE Transactions on Mobile Computing, 2008.

[2] Jing Dong, Kurt Ackermann and Cristina Nita-Rotaru "Secure group communication in wireless mesh networks", Elsevier, AdHoc Networks, 2009.

[3] Ian F.Akyildiz and Xudong Wang, "A Survey on Wireless Mesh Network", IEEE Radio Communication, 2005.

[4] Muhammad Shoaib Siddiqui and Choong Seon Hong, "Security Issues in Wireless Mesh Networks", IEEE International Conference on Multimedia and Ubiquitous Engineering, 2007.

[5] Yi Ping, Xing Hongkai, Wu Yue and Li Jianhua, "Security in Wireless Mesh Networks: Challenges and Solutions", Information Technology New Generations Sixth International Conference, pp-423-428, 2009.

[6] Muhammad Shoaib Siddiqui, Syed Obaid Amin and Choong Seon Hong, "On a Low Security Overhead Mechanism for Secure Multi-path Routing Protocol in Wireless Mesh Network", In Proceedings of Springer APNOMS, 2007.

[7] Cristina Neves, Fonseca and Instituto Superior Tecnico, "Multipath Routing for Wireless Mesh Networks",

[8] Naouel Ben Salem and Jean-Pierre Hubaux, "Securing Wireless Mesh Networks", IEEE Wireless Communication, vol-13, pp-50-55, 2006.

[9] Md. Shariful Islam, Young Yig Yoon, Md. Abdul Hamid and Choong Seon Hong, "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network "ICCSA, Vol-1, pp-972-985, 2008.

[10] Zonghua Zhang, Farid Na¨ıt-Abdesselam, Pin-Han Ho and Xiaodong Lin, "RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", IEEE Wireless Communications and Networking Conference, 2008.

[11] Wei Wang, Student Member, Xin Liu and Dilip Krishnaswamy, "Robust Routing and Scheduling in Wireless Mesh Networks under Dynamic Traffic Conditions", IEEE Transactions on Mobile Computing, 2009.

[12] Byung Joon Oh and Chang Wen Chen, "A Cross-Layer Adaptation Hcca Mac for QoS Aware H.264 Video Communications Over wireless Mesh Networks", Circuits and Systems(ISCAS), Proceedings of 2010 IEEE International Symposium,June,2010.

[13] Yuhuai Peng, Lei Guo,Qiming Gai, " Cross Layer QoS-Aware Routing Protocol for MultiRadio Multi-Channel Wireless Mesh Networks", Communication Technology (ICCT),2012 IEEE 14th International Conference,Nov 2012.

[14] Narayan D G, "A Novel Cross Layer Routinutig and Interface Assignment in Multi-Radio Wireless Mesh Network",Advances in Computing,Communications and Informatics(ICACCI),IEEE,Aug 2013.

[15] Hongfeng Wang Dingding Zhou Shi Dong, " Cross Layer Optimization Routing Algorithm for Wireless ADHOC", International Journal of Smart Home, Vol.9,No 7 (2015).pp. 169-180.

[16] Shafiullah Khan and Jonathan Loo, "Cross Layer Secure and Resource Aware On Demand Routing Protocol for Hybrid Wireless Mesh Networks", Springer, 2010.