

## ESFBR- Enhanced secure field based routing in wireless mesh networks

Fahad T. Bin Muhaya<sup>1,2</sup>, Fazl-e-Hadi<sup>2</sup> and Atif Naseer<sup>2</sup>

<sup>1</sup>Management Information System, College of Business School,

<sup>2</sup>Prince Muqrin Chair for IT Security (PMC),  
King Saud University, Kingdom of Saudi Arabia  
fmuhaya@ksu.edu.sa, fhadi@ksu.edu.sa

### Abstract

Wireless mesh network is a new type of network in which each node is connected to other nodes to enhance network reliability and performance. As compared to routing in other networks, wireless mesh network faces a lot of problem. Routing in wireless mesh network is a challenging task. Field based routing uses a little information to route the packets in the network. Due to this characteristic, field based routing algorithms are less expensive and much effective, but such algorithms also face different types of security attacks. In this paper, a novel Enhance Secure Field Based Routing Algorithm (ESFBR) is proposed which is an extension to the existing secure field based routing algorithm. ESFBR has been comprehensively tested using Omnet++ network identify and isolate the malicious node and to prevent the traffic flows from various attacks.

**Keywords:** Wireless mesh network, Field base routing, Security, ESFBR

### Introduction

Wireless Mesh networks (WMN) is a multi-hop wireless network like MANETS but routing problem in mesh networks is different because of its uniqueness from other networks (Akyildiz *et al.*, 2005; Bruno *et al.*, 2005). A Mesh Network is made up of mesh routers and mesh clients. Due to the availability of multiple paths in wireless mesh networks, connectivity with other nodes is not a big issue. Wireless Mesh Networks are reliable because every node in the network communicates with every other node for guaranteed transmission. Each wireless node can be equipped with multichannel, and each of the links can be configure to a different channel to raise network capacity (Yang *et al.*, 2005). As the mesh network becomes suitably small and cheap, it will have major applications in our daily life (Lenders *et al.*, 2006).

Mesh networks are similar to wireless networks that use superfluous and disseminated nodes for providing better reliability and range for given wireless network (Akyildiz *et al.*, 2005). In the recent years, due to the decentralized nature of wireless ad hoc networks, there has been a great increase in its demand for access to different resources (Mihail, 2008).

Mesh networks are comparatively suitable and applicable in city wide scenarios. Anycast, geocast and multicast are some of the significant applications for the group communication networks. Mesh networks are self healing, capable of routing signals efficiently and continue its working even when some nodes in the network no longer operate. For a network to function routing is one of the crucial components, hence it is more vulnerable to attacks. Besides forwarding, it is also the process through which forwarding tables are built that allows the packets to reach the correct destination. Various issues that the routing protocol must address includes, ensuring the absence of loops, detecting node failure, minimizing the

overhead network traffic and so on (Naouel Ben Salem & Jean-Pierre Hubaux, 2006). Field based routing uses a little information to route the packets. The field based routing approach has been studied in a number of different application scenarios. For instance, the approach has been used for anycast routing (Mihail *et al.*, 2008), density based routing (Curtmola & Nita-Rotaru, 2007), service discovery in mobile ad hoc networks (Dong *et al.*, 2005), sensor networks (Guangsong, 2007).

### Related work

Anycast One of the most challenging issues in wireless networks is security and much has been discussed about these issues in literature. Wireless mobile hosts are the basis of wireless multihop network which forms a temporary decentralized network. Every hop in the network is a router and two nodes that are not directly connected wants to communicate; they can communicate with each other if the other nodes between them are ready to forward packets for them (Mihail, 2008).

Some authors like (Cheng *et al.*, 2006) discussed about routing in multi-hop wireless networks that involve the indirection from a persistent name (or ID) to a locator. Concepts such as coordinate space embedding help to reduce the number and dynamism complexity of bindings and state needed for this indirection. Routing protocols which do not use these concepts often tend to route packets during route discovery or dissemination, and hence have limited scalability. In this study, Orthogonal Rendezvous Routing Protocol (ORRP) for meshed wireless networks is discussed. ORRP is a lightweight, but scalable routing protocol utilizing directional communications to relax information requirements such node localization. The ORRP source and ORRP destination send route discovery and route dissemination packets respectively in locally-chosen orthogonal directions. Connectivity happens when these paths

intersect (i.e. rendezvous). The study shows that ORRP achieves connectivity with high probability even in sparse networks with voids. The entire state information required is  $O(N^3=2)$  for N-node networks, and the state is evenly distributed. The price paid by ORRP is sub optimality in terms of path stretch compared to the shortest path, characterize the average penalty and find that it is not severe.

Mosko *et al.* (2006) proposes a new hop-by-hop routing protocol for ad hoc wireless networks that use a novel sequence number scheme to ensure loop-freedom at all times. The author uses a single large per-destination label space to order nodes in a topological sort (directed acyclic graph). Nodes manipulate the label set in network without needing destination-controlled resets, so path repair is localized. The label size is large enough that it should never be exhausted in the lifetime of any given network. Route request flooding is performed through a new method that exploits the inherent partial order of the network, so nodes can share RREQ floods. Whereas most of previous route request pruning techniques create a request tree, the new technique creates a directed acyclic request graph. Simulation results compared to AODV, DSR and OLSR show that the new protocol has in most cases equivalent or better packet delivery ratio and latency, but with a fraction of the network load.

Baumann *et al.* (2007) proposed a solution that how to routing packets into wireless Mesh networks. Routing packets into a wireless Mesh network is different from routing packets out. Because, for routing packets out of a wireless Mesh network only a single destination has to be maintained, the default route to the gateways. In contrast, for routing packets into a wireless mesh network, a proper route has to be maintained for every single node in the Mesh. The authors compared three different methods for routing packets into a wireless Mesh network. They showed that a proactive field based routing outperforms all others with respect to the packet delivery ratio while wireless Mesh gateway routing is the most scalable to the network size and still has a very high packet delivery ratio. The problem arises that how to route packet from the wireless Mesh network gateway to the Mesh nodes, specifically when route in wireless network is unstable.

Atif *et al.* (2009) discusses secure field based routing approach to route the packet securely from gateway to the network. In this approach every node calculates its field value and on the basis of these value node forwards the packet to their neighbors. In the previous approach, a node does not maintain information about field value of all the nodes so it is difficult to highlight the intruder node. In this approach, an array is introduced which shows the authenticity of node. The traffic is routed from gateway to the network in anycast, unicast and geocast manner.

### **Proposed Enhanced Secure Field Based Routing**

#### *Network model*

A WMN is made up of mesh clients and mesh

routers. Mesh routers require less transmission power as compare to other networks. The basic network architecture of WMNs is shown in Fig.1 (Waharte & Boutaba, 2005).

In WMNs, mesh clients can also work as routers because they have the potential to route packets but these clients do not work as gateways (Akyildiz *et al.*, 2005). In comparison with ad hoc networks WMNs do not strictly impose the infrastructureless property. The infrastructure of wireless mesh networks contains some fixed nodes that act as a backbone to provide connectivity to the internet.

In WMNs some fixed access points are present which provide connectivity to the wireless mobile nodes. All the nodes in the network can act as a router. The scenario of WMNs in which the ESFBR approach has been implemented and discussed is shown in Fig. 2.

In this scenario all the nodes are assumed to be fixed and also act as a router. All the traffic always route from gateway to the mesh nodes in a multihop fashion. All the node have the capability to maintain an array having information about field value of all the nodes so that when an intruder comes it should authenticate on two basis one from license and secondly from that array. If an intruder has an authenticated license but not that array the node will not forwards the packet to that intruder.

#### *Types of Nodes*

In a WMNs scenario, a gateway is shown that has routes the traffic from internet to mesh network. There are multiple types of traffic that flows from gateway to the mesh network. The second types of nodes are called intermediate nodes act as a router to route the packet to their neighbors. The third types of nodes are called group heads. They can also act as intermediate nodes and can route the packet to their neighbors but having an extra functionality to register all the other clients and can also communicate with other group heads. The fourth types of nodes are called group members that are registered members of group head.

#### *Types of Traffic*

Three types of traffic travel in the proposed network model. The first type is of anycast packets that have no fixed destination and can route to any of the group depending upon the field value. The second type of packets route in the network are called Unicast traffic that has fixed destination and always route towards fixed destination node. The third types of packets are of geocasting. They travel in a unicast manner from gateway to the group head and then the group head broadcast the message to all the members.

#### *Routing criteria*

Every node in the network calculates its routing field value from its neighbors nodes. In the proposed scenario the group head has the highest value, and the nodes directly connected to the group head have the largest field value. All the nodes calculate their field value from their directly connected neighbors. The packet always

Fig.1. Basic mesh network architecture

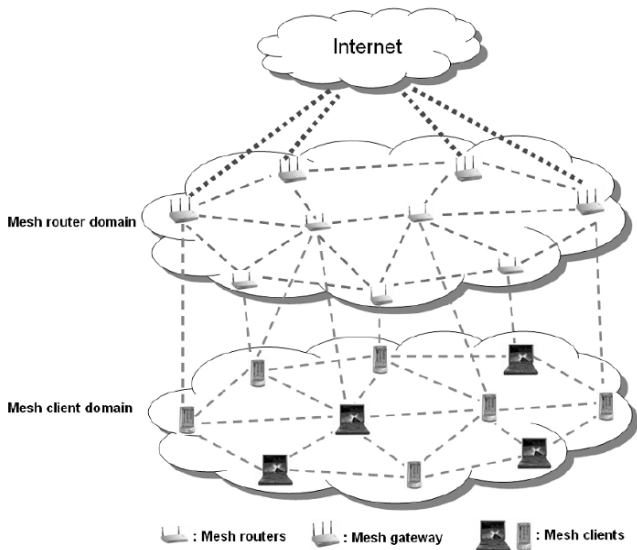


Fig.3. ESFBR vs Reactive hop by hop routing

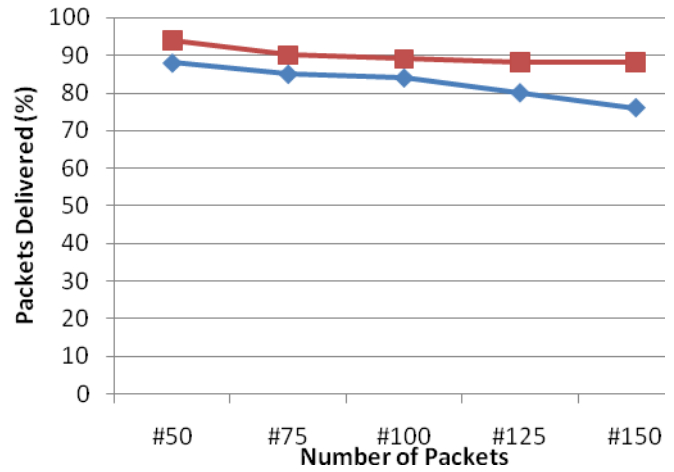


Fig.2. Basic mesh network architecture for ESFBR

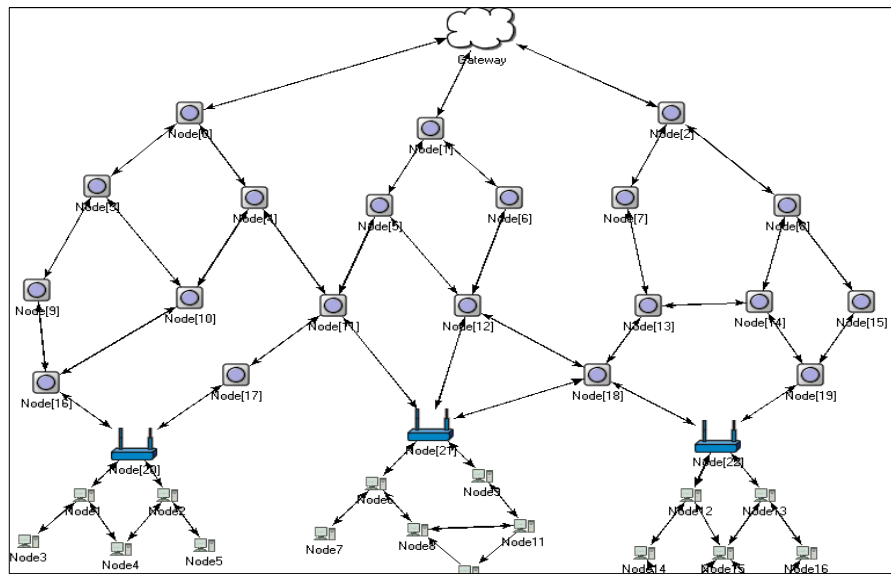


Fig.4. ESFBR vs Proactive field-based routing

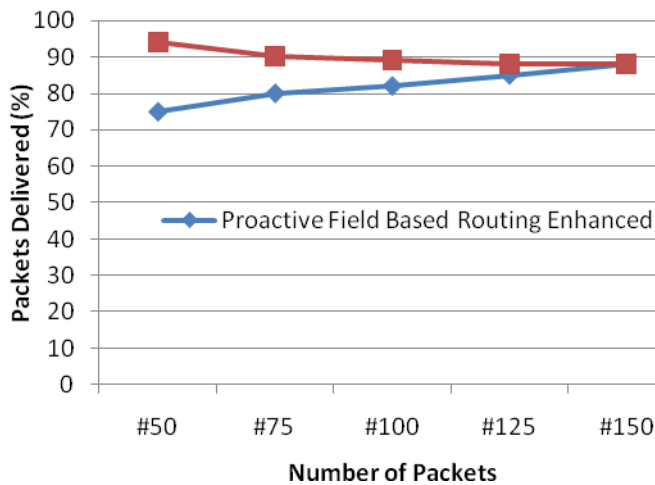
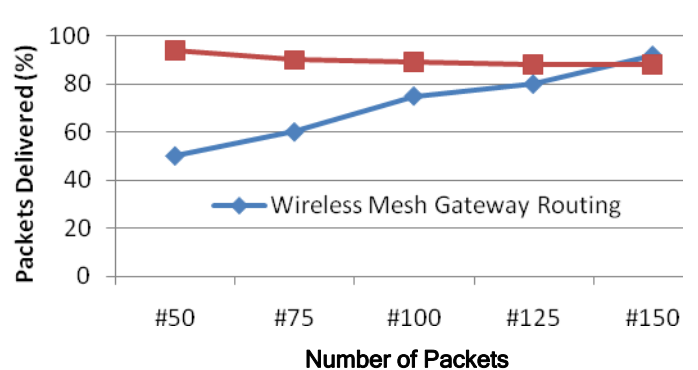


Fig.5. ESFBR vs wireless mesh gateway routing



sent to the node having highest field value. In the proposed scheme the node also maintains an array of field values so that whenever a node forwards the packets towards highest field value node it also checks weather this node have an array of filed values which shows the authenticity of that node. Although it stores an extra array but the ratio of packet delivery and security of the network increases.

Gateway routes three types of packets, the unicast, anycast and geocast. The unicast packets always travel towards a fixed destination and consider only those nodes having highest field values. The any cast packets travel towards the group head having the shortest path but the criteria is to route the packet towards highest field value node. The node always forwards the packet to the directly connected neighbor having the highest field value.

#### *The Enhanced Secure Field Based Routing (ESFBR) Approach*

The enhance secure field based routing is an extension to the existing field based routing approach. The approach shows how to initialize and calculates the field value of every node.

As discussed by Atif *et al.* (2009) when a network is populated, every node in the network calculates its field value from all of its neighbors. It then advertises their field values to all the neighbors node on the basis of which a packet is forwarded to neighbors. The packets always forwards to the authenticated nodes. Every node first authenticates its neighbors and then forwards the packet. Every node in the network has a certificate assigned by the gateway. In SFBR a node is authenticated only by its neighbor's node. But in ESFBR an array is introduced globally whose values are updated containing all the field values of its neighbors node. As packet is always forwards to the nodes having highest field value so to authenticate that node is very important. The node who is a certified member should have an array intruder announces its field value highest than any node. If the node is authenticated it must have an array containing information about all authenticated neighbors and node having intruders never have that array. So the packet will forward the node having highest field value and array of authenticated neighbors and ultimately the packet will reach to its destination.

The algorithm shows the ESFBR routing approach in wireless mesh networks. As every node authenticates its neighbors before forwarding the packets so this approach is much secure with higher packet delivery ratio.

1. ht - Field table
2. ih - initial Field Value
3. fn - find neighbor
4. fi - neighbor node
5. fp - neighbor node
6. hl - Field level
7. HL—Total Field Value
8. do

9. check node authenticity → au
10. if au is NO, then
11. remove fi
12. else
13. calculate hl level
14. exchange Field level info with fi, fp
15. update fi → ht
16. calculate the hl, fi, fp
17. end if
18. fi |fp → hl
19. forward message
20. reached destination until (destination reached)

#### **Performance evaluation**

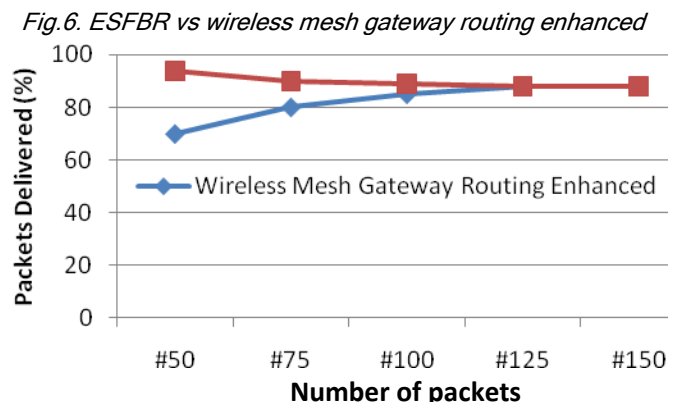
The proposed (ESFBR) scheme has been implemented and analyzed in the network simulator Omnet++ (Omnet Retrieved Jan 05, 2011, from <http://www.omnetpp.org>). It comprises of a wireless mesh network having 23 fixed nodes and a gateway to route the packet outside of a network.

The Fig.3 shows the comparison between ESFBR and Reactive hop by hop routing approaches. The ESFBR techniques show better packet delivery ratio as compared to other approach. When number of packets reaches above 100 the delivery ratio of ESFBR is much better as compared to less number of packets.

The Fig.4 shows a comparison between ESFBR and Proactive Field Based routing. ESFBR shows better packet delivery ratio with less number of packets but as the traffic increases both of them have almost same packet delivery ratio.

Fig.5 shows a packet delivery comparison between ESFBR and Wireless Mesh Gateway Routing. The ESFBR technique shows a great performance with lower number of packets but Wireless mesh gateway shows better packet delivery ratio with highest number of packets.

Fig.6 shows a packet delivery comparison between ESFBR and Wireless Mesh Gateway Routing Enhanced. The ESFBR technique show a great performance with lower number of packets but Enhanced Wireless Mesh Gateway Routing shows better packet delivery ratio with highest number of packets.





## Conclusion

Routing wireless mesh network is always prone to various types of attacks. The paper demonstrates the field based routing which uses a little information to route the packets in the network. A novel Enhance Secure Field Based Routing Algorithm (ESFBR) is proposed which is an extension to the existing secure field based routing algorithm. This technique is presented with a confidence to secure the WMNs from internal and external attacks. ESFBR has been comprehensively tested using Omnet++ network identify and isolate the malicious node and to prevent the traffic flows from various attacks. Results are encouraging. We will test more realistic scenarios in our future work.

## References

1. Atif Naseer, Younus Javed M, Fazl-e-Hadi (2009) SFBR- A Secure Field Based Routing Approach for Wireless Mesh Networks. In: Proc. of IEEE ICT & KE.
2. Cheng B.-N, Yuksel M and Kalyanaraman S (2006) Orthogonal rendezvous routing protocol for wireless mesh networks. In: Proc. of ICNP. Santa Barbara, California: IEEE.
3. Guangsong Li (2007) An Identity-Based Security Architecture for Wireless Mesh Networks. IEEE-IFIP.
4. Akyildiz I, Wang X and Wang W (2005) Wireless mesh networks: a survey. *Computer Networks* 47 (4), 445-487.
5. Dong Jing, Kurt Ackermann and Cristina Nita-Rotaru (2005) Secure group communication in wireless mesh networks. ICSTMeshNets.
6. Mihail Sichitiu L (2008) Wireless Mesh Networks Challenges and Opportunities. *ACM Computer Commun.* 31 (7), 1413-1435.
7. Mosko M and Garcia J. J.-Luna-Aceves (2006) Ad hoc routing with distributed ordered sequences. In: IEEE INFOCOM 2006, Barcelona, Spain, April.
8. Naouel Ben Salem and Jean-Pierre Hubaux (2006) Securing Wireless Mesh Networks. *IEEE Wireless Commun.* 13 (2), 50-55.
9. Bruno R, Conti M, and Gregori E (2005) Mesh networks: Commodity multihop ad hoc networks. *IEEE Commun. Magazine*, March, pp. 123-131.
10. Curtmola R, Nita-Rotaru C (2007) BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks. In: IEEE SECON 2007.
11. Baumann Rainer, Vincent Lenders, Simon Heimlicher and Martin May (2007) HEAT: Scalable Routing in Wireless Mesh Networks using Temperature Fields. *IEEE WoWMoM*.
12. Lenders V, May M and Plattner B (2006) Density-based vs. Proximity-based Anycast Routing for Mobile Networks. In: IEEE INFOCOM, Barcelona, Spain.
13. Yang Yaling, Jun Wang and Robin Kravets (2005) Designing Routing Metrics for Mesh Networks. *IEEE Workshop on Wireless Mesh Networks (WiMesh)*.
14. Waharte S and Boutaba R (2005) Tree Based Wireless Mesh Network Architecture: Topology Analysis. *ICST-MeshNets*.