academicJournals

Vol. 9(10), pp. 414-420, 30 May, 2014
DOI: 10.5897/SRE11.970
Article Number: EFAFE7744899
ISSN 1992-2248 © 2014
Copyright©2014
Author(s) retain the copyright of this article
http://www.academicjournals.org/SRE

Scientific Research and Essays

Full Length Research Paper

Secure anycast routing in wireless mesh networks

Fazl-e-Hadi[1]*, Abid Ali Minhas[1,2], Atif Naseer[3] and Abdulaziz Almazyad[2,4]

[1]Department of Computer Science, Bahria University, Islamabad, Pakistan.
[2]Al Yamamah University, Kingdom of Saudi Arabia.
[3]Riphah International University, Islamabad, Pakistan.
[4]King Saud University, Kingdom of Saudi Arabia.

Received 25 May, 2011; Accepted 16 August, 2011

Wireless Mesh Networks (WMNs) are the hybrid networks having fixed infrastructure of gateways to provide the Internet connectivity to its fixed or mobile clients. It has redundant links to provide reliable communication. Anycast is an important service for the group communication. Field based routing is getting popularity due to its robustness and simplicity. In this paper, we have studies on the security issues for the anycast service based upon the field based routing. The scheme has been studied to eliminate the effects of the external intruders and also against the internal selfish nodes. The modified secure field based routing strategies have been proposed to safeguard the legitimate traffic from these external and internal intruders. The simulation results in OMNet++ simulator shows that the proposed techniques outperform the normal routing mechanisms.

Key words: Anycast, field base routing, security.

INTRODUCTION

Wireless Mesh Networks (WMN) is a multi-hop wireless networks like MANETs, the change in structure and behavior of mesh network make the routing mechanism relatively different as compared to other networks (Akyildiz et al., 2005; Bruno et al., 2005). A mesh network consists of mesh routers and mesh client. Wireless mesh network is a multihop network so connectivity is not a big issue as compared to other networks. Various nodes perform two way communications to facilitate the reliable communication. The devices are equipped with multi channel and have the capability to handle multiple network connections (Yling et al., 2005). As the mesh network becomes small and cheap, it will easily be incorporated with a variety of devices in our everyday lives (Lenders et al., 2006). Anycast is a service which can increase service availability. It is a special type of routing in which a packet transmits to any node among a group. This single destination node may be chosen by different types of parameters like number of hops, delay or other metrics. There are set of anycast destination nodes. Anycast is used to get the service from any nearest server without considering the particular one (Ling et al., 2009). Field based routing is widely adopted due to its robustness and simplicity. We have also used the field based routing for the anycast routing in wireless mesh networks. Filed based routing is prone to various internal and external intruders' attacks. As it depends solely on a routing filed; any intruder may mislead the nodes towards itself by introducing the maximum routing filed wrongly. Wired network uses traditional approaches to achieve privacy like cryptography (Chaum et al., 1981; Reed et al., 1998; Dingledine et al., 2004) or redundancy to achieve communication end privacy (Reiter and Rubin, 1998).

The traditional approaches (Xiaoxin et al., 2009) cannot be directly applied to field base routing mechanism. That

*Corresponding author. E-mail: fhadi76@yahoo.com

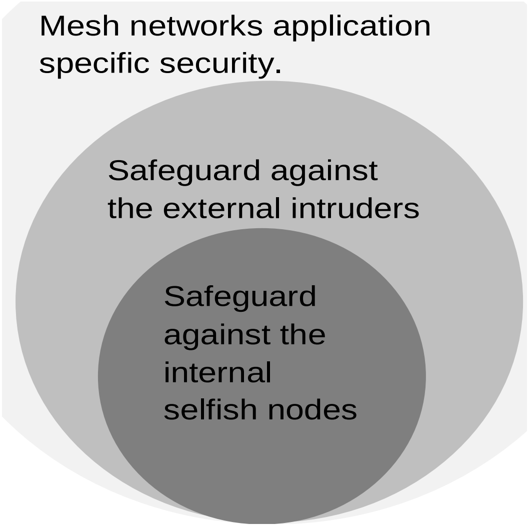
Mesh networks application specific security.
Safeguard against the external intruders
Safeguard against the internal selfish nodes

Figure 1. Wireless mesh network security architecture.

is why there is need to propose the security measures to secure the field based routing for anycast routing in wireless mesh networks.

Related work

Mesh network is a multihop network in which very node can communicate with each other using multi hops. To route the packet securely in a mesh network, every node should be well secured and route the packet securely from source to destination. To ensure that every node in the network forward the message correctly, a mechanism is needed to ensure the authenticity of a node. Literature discusses a lot about security issues in multihop wireless mesh network. In Baumann et al. (2007), authors discussed routing in large scale wireless mesh network using temperature fields. As this technique uses field based routing so need more security and authenticity of node. Sangsu et al. (2009) proposed a load balancing mechanism for any cast wireless mesh network but not discusses about the security issues related to these type of network. Ling et al. (2009) and Song and Xia (2009) discusses about any cast routing in wireless mesh network using multi gateways. As this network route packet efficiently due to any casting so need more security and reliability, yet no security mechanism is developed for these types of network. Pal and Nasipuri (2010) discuss 'quality aware anycast routing protocol' for wireless mesh network, they proposes a heuristic for route selection that tries to perform gateway and route selection to minimize interference. This study also does not focus on security issues related to this anycast routing mechanism. Anycast routing in mesh network need a lot of focus regarding security. Lebbe et al. (2007) proposes a mechanism to detect the danger in mesh network. They identify and classify the network dangers and take necessary actions to overcome those dangers. For the classification task, they apply self-organizing maps (SOMs) as the classifier to classify the danger levels in mesh network. Their study shows the danger level but discuss the counter measure and how to safe the network from different internal and external attacks. In Glass et al. (2009), authors discussed an intrusion detection mechanism that identifies man-in-the-middle and wormhole attacks against wireless mesh networks by external adversaries. Beside these, various other authors have discussed the security in such environments as this (Scarlata et al., 2001; Stephen et al., 2009).

Atif et al. (2009) discusses about 'secure filed' based routing in 'mesh network' but this technique only secures the network from external attacks. In this approach the network assumes all the nodes to be the registered members of the network and only detect the nodes coming from outside the network and shows that they are not part of the network. The nodes that are not part of the network, the mechanism declares those as a corrupt nodes and never route the traffic towards these nodes. Muhaya et al. (2010) discussed about selfish node detection as internal intruders and proposes a mechanism to identify these types of nodes.

Marti et al. (2000) proposed a mechanism watchdog to solve the problem of how to monitor the forwarding of data message. This mechanism only works for single hop network and not covers the multihop network. Also it discusses how to protect the data message but not discuss how to detect the corrupt nodes in the network. The secure routing protocol for example 'secure DSR' (Kargl et al., 2005), Ariadne (Hu et al., 2002), ARAN (Sanzgiri et al., 2002) and 'secure AODV' (Zapata, 2002) provide secure mechanism to maintain in which no nodes will come as an intruder. All these types of algorithms not detect the misbehavior of internal nodes.

NETWORK MODEL

Mesh network faces a lot of security threats like internal, external, application security and different types of group head attacks. External attacks are launched by the external intruders hijacking the sessions and capture the data to launch the active and passive attacks. Internal attacks are launched by the internal legitimate selfish clients to mislead the routing traffic and to launch various attacks. In this paper, we have covered all the aspects of external and internal attacks. The detailed analysis has been presented for anycast traffic type. Moreover some results have been confirmed for multimedia traffic as well.

An anycast scenario of mesh network is proposed showing some nodes connected in a mesh style having a gateway and routers. All nodes in a network act as a router.

Security architecture

The wireless mesh network security architecture is given in Figure 1.

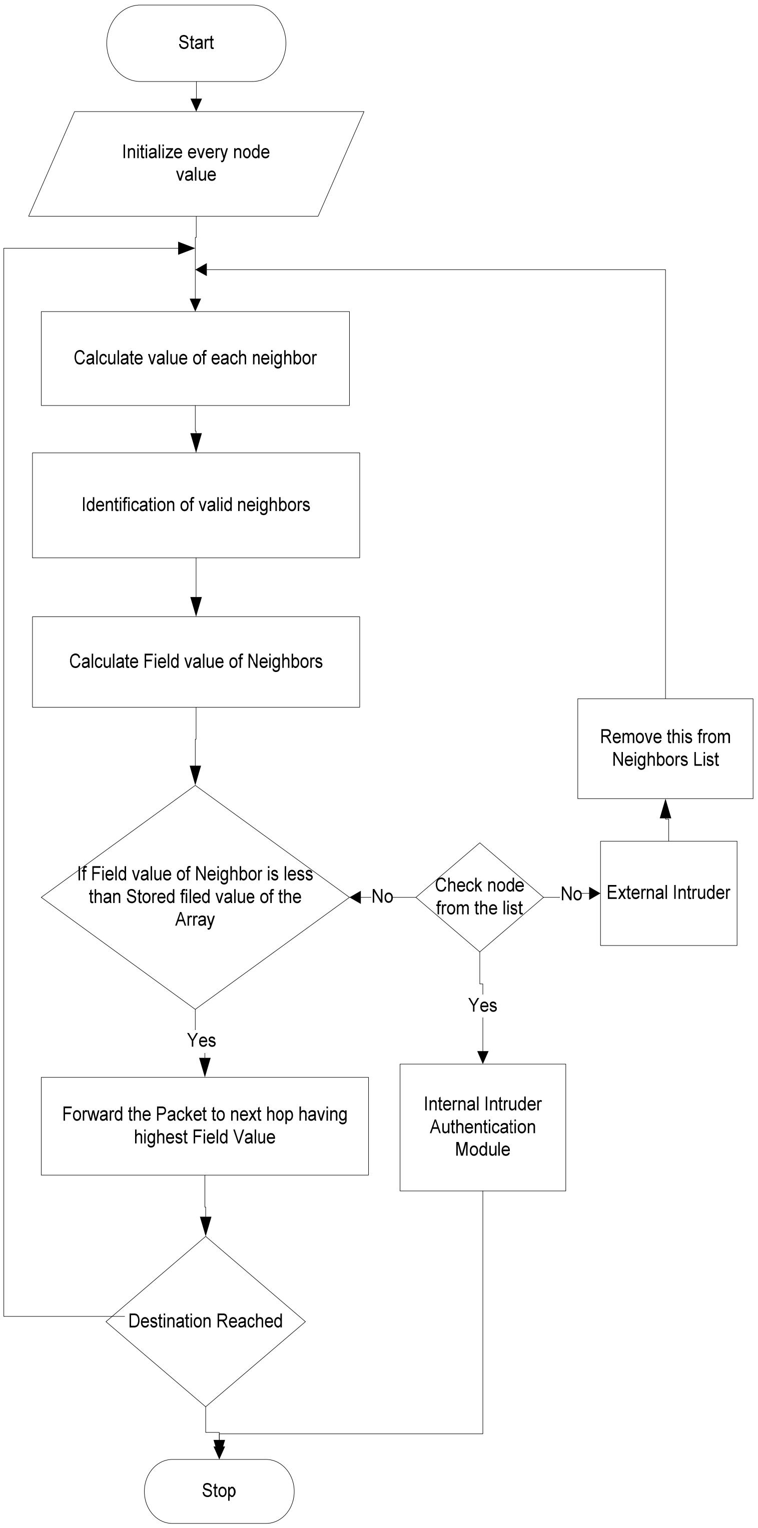
Start
Initialize every node value
Calculate value of each neighbor
Identification of valid neighbors
Calculate Field value of Neighbors
If Field value of Neighbor is less than Stored filed value of the Array
No
Check node from the list
No
External Intruder
Remove this from Neighbors List
Yes
Yes
Forward the Packet to next hop having highest Field Value
Internal Intruder Authentication Module
Destination Reached
Stop

Figure 2. Flowchart for detecting external attacks.

Flow charts

To mitigate various external and internal attacks, detailed Flow charts are given in Figures 2 and 3 respectively. Figure 2 shows the flow chart of detecting the external attacks on mesh network. As each node calculates their field value and share this value with directly connected neighbors; every node calculates its value from their

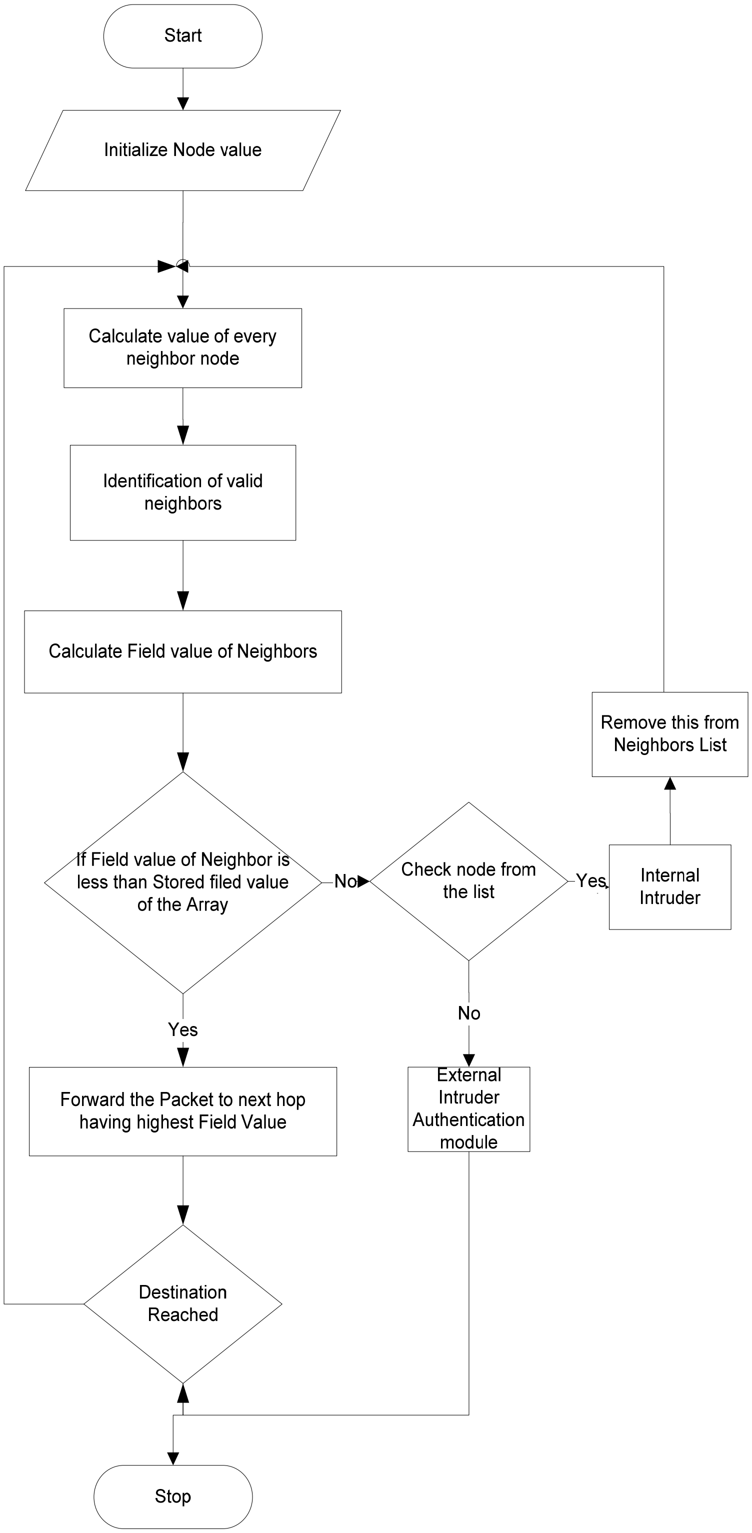
Start
Initialize Node value
Calculate value of every neighbor node
Identification of valid neighbors
Calculate Field value of Neighbors
If Field value of Neighbor is less than Stored filed value of the Array
No
Check node from the list
Yes
Internal Intruder
Remove this from Neighbors List
No
External Intruder Authentication module
Yes
Forward the Packet to next hop having highest Field Value
Destination Reached
Stop

Figure 3. Flowchart for detecting internal attacks.

neighbors and performs routing on the basis of these values. If the value of neighbors is less than the node value, now it will be authenticated as an internal or external intruder. The node first check from the list if it does not exists as registered and behaves like a normal node and advertises its value to be maximum so that

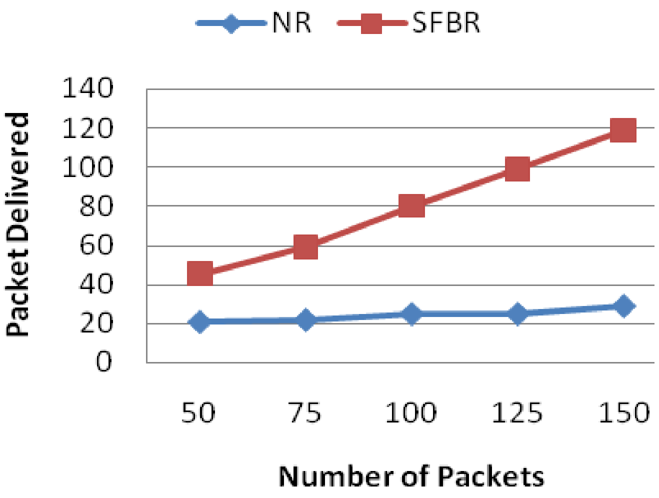

Figure 4. Packets delivery ratio by intruders at various level.

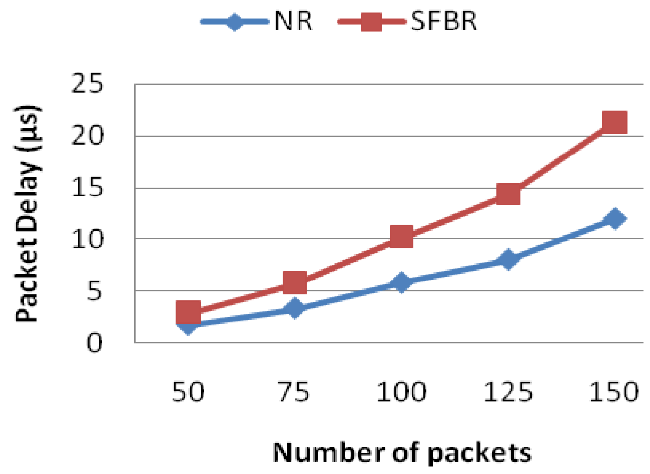

Figure 5. Total packet delay time (µs).

routing always takes place by this node, the node never forwards the packet and declares it as an external intruder. Figure 3 shows the flow chart of detecting the internal attacks on mesh network. As each node calculates their field value and share this value with directly connected neighbors. Every node calculates its value from their neighbors and performs routing on the basis of these values. If the value of neighbors is less than the node value, now it will be authenticated as an internal or external intruder. The node first check from the list if it does not exist as a registered node and still behaves like an intruder, the node never forwards the packet and declare it as an intruder.

PERFORMANCE EVALUATION

The performance of secure field based routing (SFBR) is measured using the OMNet++ simulator. The results

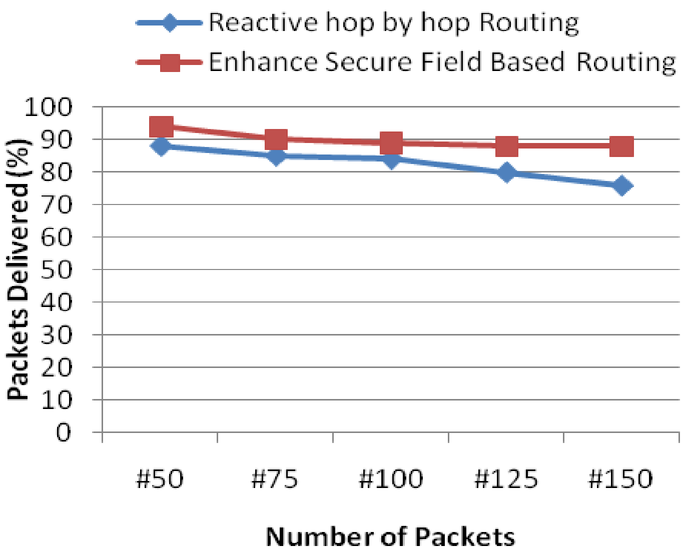

Figure 6. ESFBR vs reactive hop by hop routing.

shown in Figure 4 explain the packet delivery of packets at different samples of packets. This graph shows a comparison between secure and normal routing packet delivery. The secure mechanism shows greater packet delivery ratio as compared to normal routing mechanism because it minimizes the probability of dropping the packets by the possible external intruders. Figure 5 shows the delay of both the normal and secure routing. As secure field based routing follow alternates path in case of any intruder so faces some delay as compared to normal routing mechanism, but normal routing compromises efficiency and suffer delay in packet delivery. After performing the secure field based routing, the enhanced secure routing mechanism (ESFBR) is used to route the packet efficiently. ESFBR uses a secure array to maintain the field value of every node, this array help in routing the packets securely. ESFBR is compared with many protocols already working. Figure 6 shows the comparison between ‘reactive hop’ by hop and ESFBR routing mechanism. ESFBR protocol experiences better packet delivery ratio as compared to ‘reactive hop’ by hop routing. Figure 7 shows the comparison of ‘proactive field’ based routing and ESFBR. ESFBR faces a better packet delivery ratio at less number of packets but as number of packets increases the ESFBR shows same number of packets delivery as in proactive field based routing mechanism. Figure 8 shows the delivery ratio of wireless mesh gateway routing and ESFBR. ESFBR is efficient at less number of packets but wireless mesh gateway routing shows better ratio at higher number of packets. Figure 9 depicts the comparison between wireless mesh gateway routing enhanced and ESFBR shows the best performance of ESFBR at lower number of packets, but as the packets increases, both protocols shows the same type of behavior. We have also performed some test for the multimedia traffic using field based routing in wireless

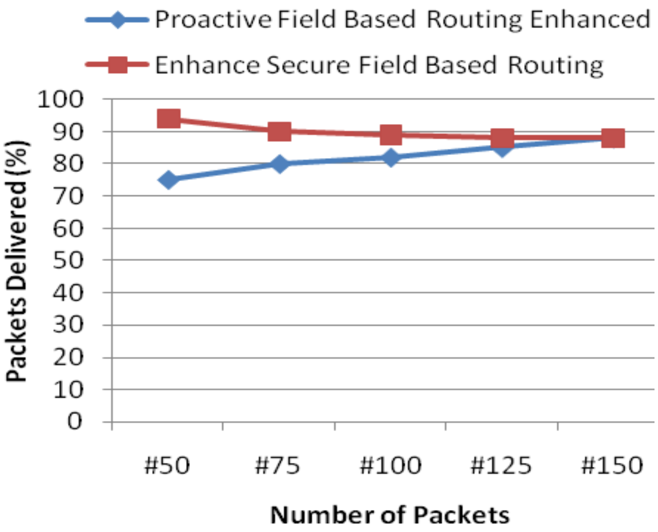

Figure 7. ESFBR vs proactive field based routing.

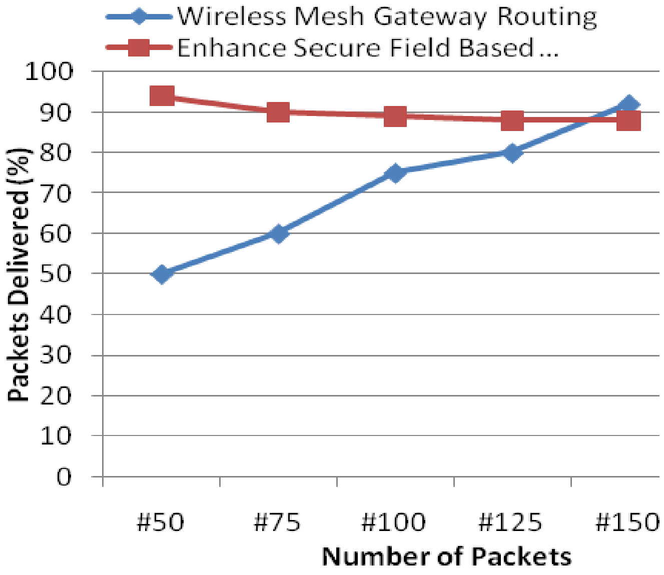

Figure 8. ESFBR vs wireless mesh gateway routing.

mesh networks. As multimedia traffic may consists of different length of packets.

The study considers different size of multimedia packet and studying the delay occurs due to change in the packet size. The behavior shows that as the multimedia packet increases in size, the delay increase. The results are shown in Figure 10. Figure 11 shows the comparison of secure and unsecure multimedia routing. Most of the traffic does not reach the destination due to unauthenticated nodes present in the network. The earlier paper proposed a secure multimedia routing and compares the results with unsecure routing in which

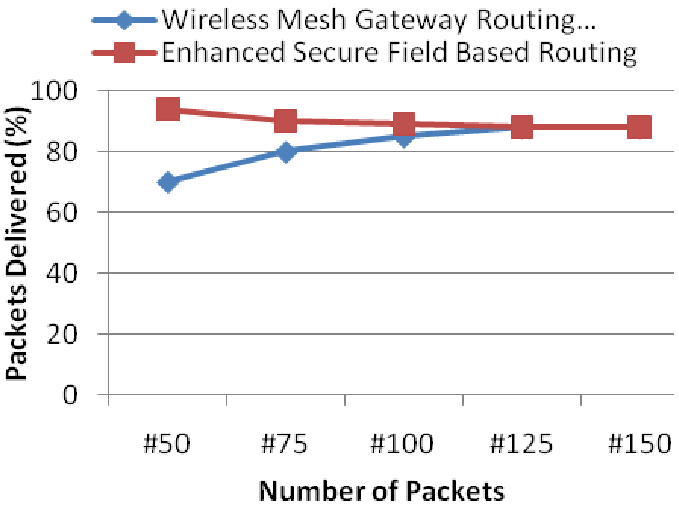

Figure 9. ESFBR vs wireless mesh gateway routing enhanced.

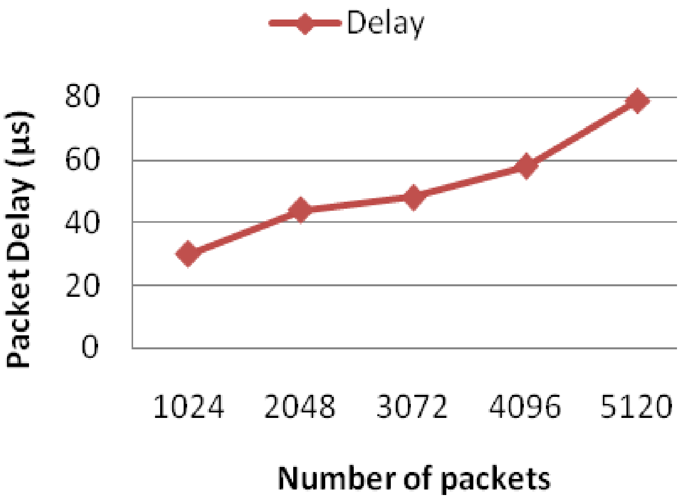

Figure 10. Delay in multimedia traffic.

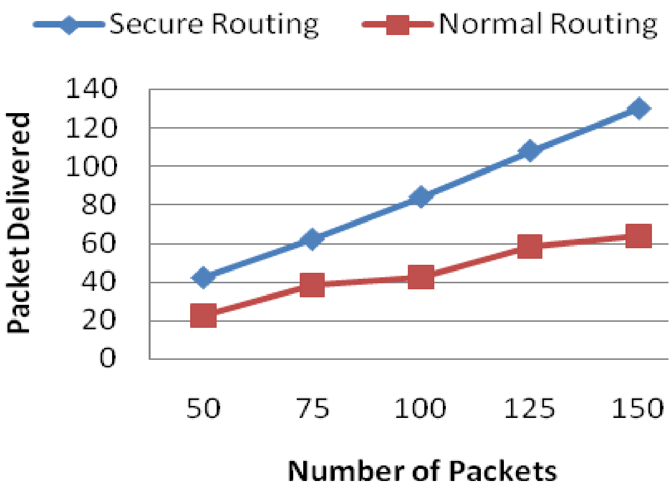

Figure 11. Packets delivery ratio with and without intruders.

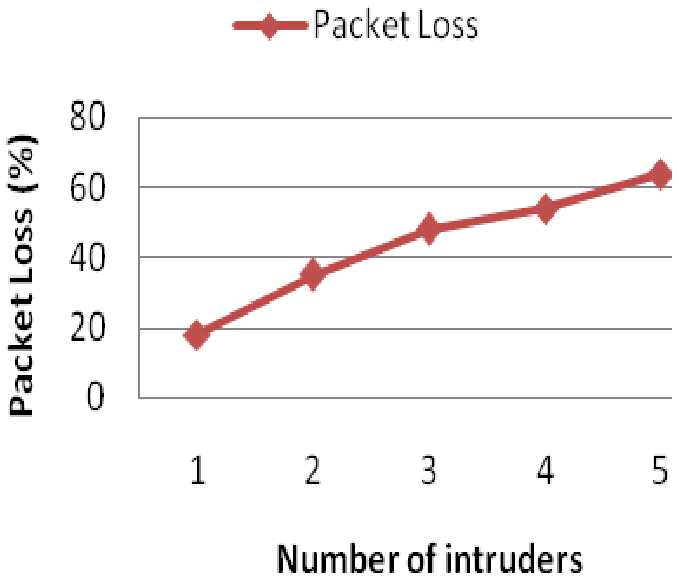

Figure 12. Packet loss due to change in number of intruders.

some intruders were present in the network. These intruders drop most of the packets and almost half of the traffic does not reach the destination. In secure routing the authentication mechanism first authenticate every node and then deliver the packet to the authenticated node. Figure 12 shows the packet loss due to change in number of intruders at different levels to analyze the behavior of the network.

CONCLUDING REMARKS AND FUTURE WORK

Field based routing in wireless mesh networks has numerous security issues. In this paper we have studied the anycast routing and the multimedia traffic based upon the field based routing. Novel approach is adopted to mitigate the external and internal intruder's attacks. Extensive simulation results revealed that the proposed techniques are secure and improves the system reliability while it keeps the best features of the field base routing.

Conflict of Interests

The author(s) have not declared any conflict of interests.

REFERENCES

Akyildiz XW, Wang W (2005). Wireless mesh networks: A survey. Comput. Netw. 47(4):445-487. http://dx.doi.org/10.1016/j.comnet.2004.12.001

Baumann R, Vincent L, Simon H, Martin M (2007). HEAT: Scalable Routing in Wireless Mesh Networks using Temperature Fields. IEEE WoWMoM.

Bruno R, Conti M, Gregori E (2005). Mesh networks: Commodity multihop ad hoc networks. IEEE Commun. Mag. pp. 123-131. http://dx.doi.org/10.1109/MCOM.2005.1404606

Chaum DL (1981).Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM 24(2): 84-88. http://dx.doi.org/10.1145/358549.358563

Dingledine R, Mathewson N, Syverson P (2004). Tor: The Second-Generation Onion Router. In 13th USENIX Security Symposium.

Hu Y, Perrig A, Johnson D (2002). Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of ACM MobiCom.

Kargl F, Geiss A (2005). Secure Dynamic Source Routing. In Proceedings of HICSS, p. 38.

Lenders V, May M, Plattner B (2006). Density-based vs. Proximity-based Anycast Routing for Mobile Networks. In IEEE INFOCOM, Barcelona, Spain.

Marti S, Giuli T, Lai K, Baker M (2000). Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of ACM MobiCom'00. http://dx.doi.org/10.1145/345910.345955

Pal A, Nasipuri A (2010). A quality aware anycast routing protocol for wireless mesh networks in IEEE southeastcon 2010 (southeastcon).

Reed M, Syverson P, Goldschlag D (1998). Anonymous Connections and Onion Routing. IEEE J. Select. Areas Commun. Special Issue on Copyright and Privacy Protection, pp. 482-494.

Reiter MK, Rubin AD (1998). Crowds: Anonymity ForWeb Transactions. ACM Trans. Inf. Syst. Secur. 1:1. http://dx.doi.org/10.1145/290163.290168

Sangsu J, Dujeong L, Malaz K, June-Koo KR (2009). Autonomous Load Balancing Anycast Routing Protocol for Wireless Mesh Networks, appeared in World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM.

Sanzgiri K, Dahill B, Levine B, Belding-Royer E (2002). A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of IEEE ICNP'.

Scarlata V, Levine B, Shields C (2001). Responder Anonymity and Anonymous Peer-to-Peer File Sharing. IEEE International Conference on Network Protocols (ICNP), Riverside, CA.

Song L, Xia Z (2009). An Anycast Routing Protocol for Wireless Mesh Access Network. WASE Int. Conference on Information Engineering.

Stephen G, Vallipuram M, Vallipuram M (2009). Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. International Conference on Advanced Information Networking and Applications.

Xiaoxin W, Ninghui L (2009). Achieving Privacy in Mesh Networks 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia.

Yling Y, Jun W, Robin K (2005). Designing Routing Metrics for Mesh Networks, IEEE Workshop on Wireless Mesh Networks (WiMesh).

Zapata MG (2002). Secure Ad hoc On-Demand Distance Vector Routing. ACM Mobile Comput. Commun. Rev. (MC2R). 6(3):106-107.