On Optimization and Security of Multimedia Communication in Wireless Mesh Networks

Fazl-e-Hadi, Fahad T. Bin Muhaya, Atif Naseer
Prince Muqrin Chair for IT security (PMC),
King Saud University, Kingdom of Saudi Arabia

Abstract

Wireless mesh networks (WMNs) are new type of networks in which every node can communicates to all neighboring nodes to enhance network reliability and performance. Network traffic cost optimization and its security in wireless mesh network is a challenging task. The concept of field based routing (FBR) is gaining popularity because it uses a little information to route the packets. These routing algorithms are robust, inexpensive and scalable. Authors believe that the FBR is the better choice for the multimedia communication in wireless mesh networks. Because FBR exchanges little information for building and maintenance of the routing tables. Regardless of robustness and scalability of the FBR it is also prone to different active and passive attacks. In this paper we first study that how multimedia communication can be done using FBR (optimization) and then take some security measures to eliminate the risk of intruder intervention in such communication. Multimedia FBR and its security has been extensively studied using Omnet++ network simulator to identify and isolate the malicious node and to prevent the traffic flows from various active and passive attacks.

1. Introduction

Unlike the traditional mobile ad hoc networks (MANETs), wireless mesh networks (WMNs) have redundant multi-hop wireless and wired links. These unique features of WMNs make the routing problem relatively different [1], [2]. Mesh network have a fixed infrastructure like the gateways to provide the internet connectivity to the wireless nodes which might have fixed infrastructure or not. Mesh routers and mesh client are the key parts in addition to the gateways. In the WMNs there are redundant paths so connectivity issue is not a problem. All nodes in the network can communicate with each other to provide reliable path. Each of the wireless nodes can be operational with multichannel, and each of the links can be configured to a range of channel to increase network capacity [3]. As the mesh network becomes adequately small and cheap, it will be easily incorporated with a variety of devices in our everyday lives [4].

Mesh network is basically an appropriate choice for the city wide networks. It has a variety of interesting applications in a city wide network scenario. In most of city wide network a number of groups exist like universities, musical groups, gaming and news etc. The individuals and the groups may want to share the information, play games, share music and other multimedia files etc. There might be a variety of traffic types like anycast, geocast and multicast which can be used for sharing of the multimedia files. Another important application in the use of this network in a crisis hazards situation. The network may be coupled with the special type of MANETs like delay tolerant network to ensure the data delivery in a sparsely distributed network nodes. Vehicular communication may be done in a city wide network and can be coupled with the WMNs traffic to route the traffic towards the internet.

Security is an important and main issue in WMNs due to some of the challenging features of WMNs, like low upfront investment, high robustness, good scalability, increased coverage etc. The unique features and redundant links which on one hand provide the reliability but on the other hand challenge the network security; openness of such networks is also prone to various attacks e.g. some of the security challenges faced by WMNs are detecting the corrupted nodes, multi-hop routing and fairness [5]. Based upon these facts security issue remains challenging for the research community. At some stages WMNs might have memory and computational limitations so the traditional schemes for achieving security are not suitable.

Field based routing got popularity because it uses tiny information for routing. The study considers the field base routing for the optimization of multimedia communication cost in first phase. Nowadays field based routing algorithms are in use due to its robustness and simplicity. Security in field based routing algorithm is still an open issue. The study also considers different active and passive attack scenarios for multimedia communication and analyzes the behavior of intruder in both type of attacks, and provides a solution to overcome these attacks. This paper is an extension of our previous

study [6] with more results and discussion. We analyze and compare the results of field based routing for multimedia communication with and without implementing the security.

2. Related work

Many researchers focus on the wireless networks for its various challenges. The main focus remains on the routing schemes. A thorough study reveals that field based routing, multimedia and its security still needs researcher's attention. Normally the wireless multihop network is based on wireless mobile hosts without a central administration. All nodes can communicate to each other; every node acts as a router to forward the routed packets towards its destination. Nodes lying in the direct range of each other may communicate directly; all this communication may takes place in an infrastructure based or infrastructure less scenario [7].

Lenders et al [8] and V. Park et al [9] proposed the field based routing in their respective papers. We used the field based routing algorithm for multimedia communication which is an inexpensive and robust method. In this way the network traffic cost is lessen which leads us towards the optimization of such traffic. As discussed earlier that contrast to the robustness of field base routing; it is prone to different security attacks. Rainer Baumann et al [10] proposed a field base routing algorithm (HEAT) for spreading the packets from the mesh nodes to the gateway via anycast routing. The routing is in fact based upon the temperature field which is calculated considering the gateway as the heat source but the security issue remains there.

Authorization, authentication, integrity and confidentiality are the security issues in MNNs which are discussed by siddiqui et al [5]. These issues are difficult to handle due to the wireless ad hoc architecture of WMNs. Khan et al [11] proposed a hybrid wireless mesh protocol (HWMP). The HWMP is a good effort but still have security imperfections in it. Another study by salem et al [12] discussed about the detection of corrupt transit access points (TAPs). As the TAPs are not restricted physically so there remain security issues due to multihop wireless communications. Securing the TAPs itself might help to detect the intruder's access but our recently study focuses on the nodes registration and securing the traffic flows through the field based routing algorithms. Same efforts are made in other networks like Wang et al [13] proposed two centralized group rekeying (CGR) schemes to secure group communication in wireless sensor networks. There are some specific issues with the wiles sensor networks which are not the issues of the WMNs e.g. WMNs have no issue of the power utilization so extensive computation may be performed at different fixed high battery powered intermediate nodes which is a bottleneck in wireless sensor networks.

A broadcast encryption scheme is proposed by kalaiselvi et al [14], which can be used for secure group communication. The scheme basically addresses the authentication for secure group communication but some of the active and passive attacks were not considered. Based on the fact that there are some unique characteristics of field based routing algorithms; this paper focuses on the requirement of some special consideration for the field base routing security and its efficient use for the multimedia communication. Another study by jin et al [15] proposed an agreement protocol which is very efficient consistent and secure but didn't discuss about the security of field based routing algorithms in which wrong advertisement of a small field can attract a large and might be an important content of multimedia traffic. There are some fundamental studies to secure the multicast protocols in WMNs [16], [17]. Data privacy in WMNs has been addressed by dong et al [18].

Based upon the above literature survey it is concluded there is a room for optimization and securing the multimedia communication based upon the field base routing algorithm; which is the focus of this paper.

3. Network model

Multimedia communication may take place between individual nodes and also it is important for the group communication. So in this way unicast, anycast multicast and geocast traffic types may be considered. Keeping the fact in mind scenario developed for the multimedia communication using field based routing algorithm which is depicted in Figure 1. In the given network there is a gateway and multiple routing nodes. Every node has the ability to route the packet to its next hop. The nodes having alike round shape are certified nodes; by certified we mean that when the network populates the certification authority which is the gateway in this case will issue a unique ID to its legitimate nodes. The list of authentic nodes is also shared among the legitimate clients. The intruders may came into the direct range of the other legitimate nodes and may launch various attacks; the intruders are depicted different shape which no certificate issued by the certification authority.

Before forwarding the packets to its next hop the node first check the certificate issued to it by the certification authority; if the node has that certificate (means if it is included in the certified node list) than it is an authenticated node and can receive the multimedia packets, but if that node have no certificate like two intruders shown in the scenario so the forwarding node will stop sending packets to it and these nodes will be declared as intruders and will

not be considered for the future forwarding decisions.

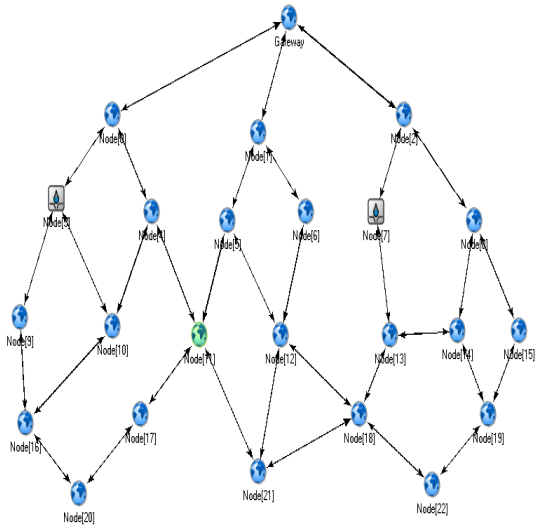

Figure 1. Mesh Network Scenario

As the field base routing is used for transmitting the multimedia traffic which minimize the routing overhead and hence minimize the transmission cost. Based on this assumption we lead towards the optimization of the traffic cost. Furthermore to the best of our knowledge no one has studies the security of multimedia communication using the field based routing in wireless mesh networks. The authors claim it as the contribution to transmit the multimedia traffic through the field based routing algorithm, which is a robust and scalable routing algorithm. Furthermore the security is such scenario has been considered to eliminate the effect of the external intruders.

The scope of the study is limited to the fixed scenario, in which the certification authority (Gateway in this case) issues the certificates which are the unique IDs when the network populates. The study focuses on the elimination of external intruders from the neighbor list while forwarding the packet to the next hop; the internal nodes may behave maliciously which can be detected by the behavior analysis which has been studied by the authors of this paper in their separate work [19].

4. Implementation and analysis

In order to analyze the proposed scheme for multimedia communication has been implemented and analyzed in the network simulator OMNet++ [20]. As shown in figure 1 the network topology use for this analysis comprising of 23 wireless nodes and a gateway that provides access to the internet. Figure 2 shows the analysis of delay occurs due to routing of multimedia packets. In this paper we studied the delay by varying the packet size. The multimedia traffic might consist of varying length of packets. The study consider different size of multimedia packet and analyze the delay occur due to change in the packet size. The behavior shows that as the multimedia packet size increases the delay increase.

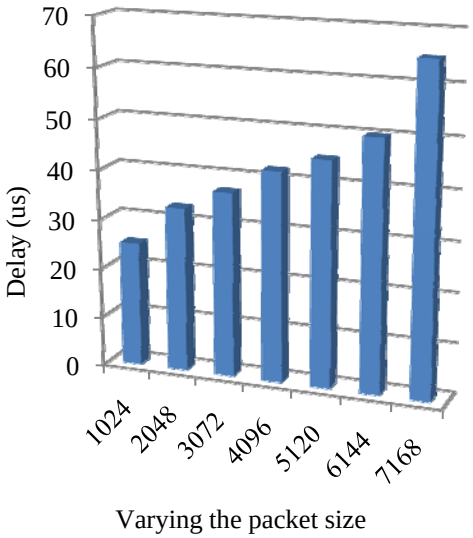

Figure 2. Delay analysis by varying the packet size

One of the main reasons of increased delay in large size packet transmission is that there might be restriction on local link like the maximum transmission unit (MTU) at physical layer. The larger packets are divided into the smaller packet according to the local MTU. The header to payload ratio increases; this cause more transmission which lead to larger delay per received packet. Figure 2 shows that the delay will increase as the size of packet increases. Hence to split a multimedia packet causes for the increase delay in the network.

The multimedia traffic has been studied by adopting the security measures and without security measures. Figure 3 shows the comparison of the packet delivery ratio of these schemes. If any intruders got access in the work than it causes the reduction in the packet delivery ratio because it can launch various active and passive attacks which lead to the delay and drop of the legitimate packets. It can block most of the traffic; it can hold various packets for the traffic analysis so a larger chunk of data couldn't reach to the destination.

As the study proposed a secure multimedia routing by authenticating the nodes and consider the legitimate nodes for the forwarding the incoming packets. We name it secure multimedia routing (SMR). The results are compared with normal routing (NR) in which some intruders came in and capture the traffic. These intruders captured most of the traffic and more or less 50% reached to the

destination and rests of the packets are dropped. In secure routing the authentication mechanism first authenticate each node and then send the packet to the authenticated node. If the node is not an authentic and don't have any certificate issued by the certificate authority then the node is black listed and not considered for the multimedia traffic. The alternate paths are taken for the packet transmission which might be lengthy but secure. The packets may experience a bit more delay due to the alternate longer paths, but the secure mechanism ensure maximum delivery of packets. The ultimate results are optimal. Few packets in secure communication may be lost due to the random link/node breakdown.

Load balancing is also handled in the planned scheme as the packets go after the alternate path. A threshold is set for the traffic measurement and whenever it reaches to the pre-defined threshold value; the traffic is diverted to an alternate path. This will increase the delay in network but distributes the traffic load equally all the way through the network.

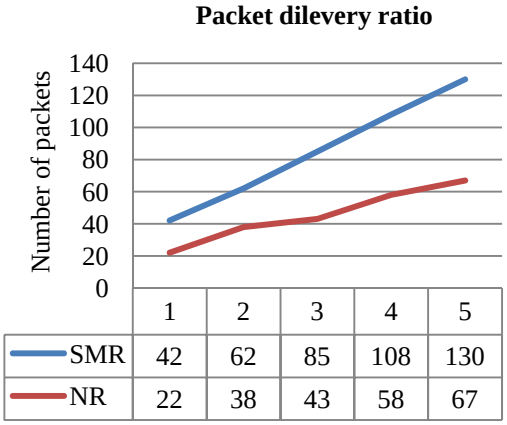

Figure 3. Packets delivery ratio comparison

There might be a number of intruders who got access in the network. The study analyzes the behavior of network by considering various intruders in the network. Figure 4 shows the number of packets lost by varying the number of intruders. We vary the number of intruders from one to five.

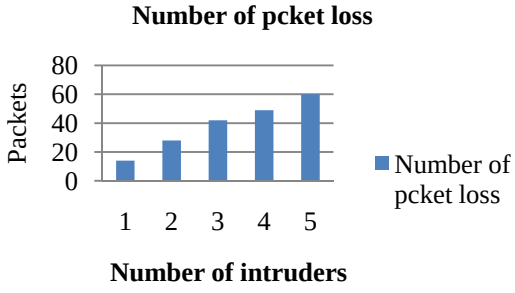

Figure 4. Packet loss varying the number of intruders.

5. Conclusion

Efficient routing, including the multimedia communication in wireless mesh network is a challenging task. The concept of field based routing (FBR) is gaining the attraction because of its less routing overhead. It uses a little information to route the packets. In this paper we first studied that how multimedia communication can be done using FBR to optimize the network traffic cost. Moreover we take some security measures to eradicate the risk of intruder interference in such communication. The study focuses on the elimination of external intruders from the neighbor list while forwarding the packet to the next hop. Extensive simulation results shows that the SMR outperforms the NR in respect of better delivery ratio and less routing delay.

6. Acknowledgement

This work is supported by the Prince Muqrin Chair for IT security (PMC), Kind Saud University, Riyadh, Kingdom of Saudi Arabia.

7. References

[1] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, vol. 47, no. 4, pp. 445–487, March 2005.

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: Commodity multihop ad hoc networks," IEEE Commun. Magazine, pp. 123–131, March 2005.

[3] Yaling Yang , Jun Wang , Robin Kravets, "Designing Routing Metrics for Mesh Networks" , IEEE Workshop on Wireless Mesh Networks (WiMesh), 2005

[4] V. Lenders, M. May, and B. Plattner, "Density-based vs. Proximity-based Anycast Routing for Mobile Networks," in IEEE INFOCOM, Barcelona, Spain, April 2006.

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

[6] Fazl-e-Hadi, Fahad Bin Muhaya, Atif Naseer, "Secure Multimedia Communication in Wireless Mesh Networks", in proc. of the 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010), November 8-11, 2010, London, UK.

[7] Mihail L. Sichitiu, "Wireless Mesh Networks Challenges and Opportunities", ACM Computer Communications, Volume 31, Issue 7, Pages 1413-1435, 2008.

[8] V. Lenders, M. May, and B. Plattner, "Density-based vs. Proximity-based Anycast Routing for Mobile

Networks," in IEEE INFOCOM, Barcelona, Spain, April 2006.

[9] V. Park and S. Corson, Temporally-Ordered Routing Algorithm (TORA), IETF Internet Draft, July 2001.

[10] Rainer Baumann and Vincent Lenders and Simon Heimlicher and Martin May, "HEAT: Scalable Routing in Wireless Mesh Networks using Temperature Fields," IEEE WoWMoM, 2007.

[11] Muhammad Ali Khan, Syed Muhammad Reza, Hamed Moradi: A Brief Overview Of Wireless Mesh Networks with Focus on Routing", IEEE-ICC, 2007

[12] Naouel Ben Salem Jean-Pierre Hubaux: "Securing Wireless Mesh Networks", IEEE Wireless Communications, vol. 13, no 2, 2006.

[13] Yong Wang and Byrav Ramamurthy: Group Rekeying Schemes for Secure Group Communication in Wireless Sensor Networks", IEEE-ICC, 2007

[14] Kalaiselvi, S. Begum, S.J. ,"a secure group communication using non-interactive key computation in multiparty key agreement", IEEE-ICCC, 2008

[15] Zhen-Ai Jin; Geum-Dal Park; Kee-Young Yoo, "An improved Secure Authenticated Group Key Agreement Protocol for WMNs", IEEE-ALPIT, 2008

[16] S.Roy, V.Addada, S. Setia, S. Jajodia, Securing MAODV: attacks and counter measures, in: proceedings of SECON'05, 2005.

[17] R. Curtmola, C. Nita-Rotaru, BSMR: Byzantine-resilent secure multicast routing in multi-hop wireless networks, in: IEEE SECON 2007.

[18] Jing Dong, Kurt Ackermann, Cristina Nita-Rotaru: Secure group communication in wireless mesh networks", ICST-MeshNets, 2005

[19] Fahad bin Muhaya, Fazl-e-Hadi, Atif Naseer, "Selfish Node Detection in Wireless Mesh Networks", IEEE-ICNIT, Philippines, 2010.

[20] http://www.omnetpp.org, Access date: Feb 5, 2011.

