Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 51A (2012) 11136-11140

ISSN: 2229-712X

Novel methods for reliable multicast routing in wireless mesh networks

B.Meenakumari and T.Preethiya

Department of Electronics and Communication Engineering, Kalasalingam UniversityAnand Nagar, KrishnanKoil-626126, India.

ARTICLE INFO

Article history:

Received: 8 February 2012;

Received in revised form:

13 October 2012;

Accepted: 27 October 2012;

Keywords

Wireless Mesh Networks,
ODMRP,
Vulnerability,
Multicast routing,
Trust key,
Packet Delivery Ratio,
Latency,

ABSTRACT

A reliable multicast routing enables a process to multicast a message to a group of clients in a way that ensures all the host destination group members receive the same message. Multicast routing on Wireless Mesh Networks brings great challenges in security due to its high dynamics, link vulnerability, and complete decentralization. Hence, due to its insufficient security requirements and vulnerability to attacks, a novel secure multicast routing protocol S-ODMRP, takes full advantage of trusted computing technology. The novel methods proposed overcomes the above degradation and decreases the communication cost by broadcasting the local traffic and by providing self healing mechanism to each nodes in the network so that it cures the link failure caused by the failed routers and reconstructs the multicast key path, in which the path selection is based on the link basis. And the trusted key is distributed for the secure multicast routing in the Wireless Mesh Networks. In which the trust value for each node is based on some set of rules such as the jointly behaviors, energy behaviors, and the activity model. Hence the NS-2 simulation includes various parameters such as Packet Delivery Ratio (PDR), Bandwidth overhead, cost per received packet, number of attackers and achieves the higher security and throughput.

Introduction

Wireless networks face security threads while transmitting the data between the sources to the destination,hence they communicate through radio transmissions, without physical connections and without peripheral cabling.Wireless Systems include local area networks, personal networks, cell phones, etc. While considering the Wireless Mesh Networks, security is the major issue. Therefore ,security is provided to the WMN Through the various cryptographic techniques such as identity based cryptography, Adaptive and Bandwidth Reducing (ABR) tree, lolus, etc., Since these cryptographic techniques also seems to be more complex in the , trust model is computed to provide security and also to increase the reliability in the Wireless Mesh Networks.

Since these cryptographic techniques also seems to be more complex in the , trust model is computed to provide security and also to increase the reliability in the Wireless Mesh Networks.

Wireless Mesh Networks

The term “Wireless Mesh Networks” describes wireless networks in which each node can communicate directly with one or more peer nodes. And the term Mesh originally used to suggest that all nodes were connected to all other nodes, but most modern meshes connect only a subset of nodes to each other. Nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router.

Security in Wireless Mesh Networks

WMNs still lack efficient and scalable security solutions, because their security is more easily compromised due to several factors: their distributed network architecture, the vulnerability of channels and nodes in the shared wireless medium, and the dynamic change of network topology. Attacks in different protocol layers can easily cause the network to fail. Attacks may occur in the routing protocol such as advertising wrong routing updates. The attacker may sneak into the network, impersonate a legitimate node, and not follow the required specifications of a routing protocol.

It has the following advantages such as it

Offers high speed wireless packet data access across a wide coverage area. Minimizes cost of capital, installation and commissioning. Utilizes low cost 802.11 technologies highly flexible in terms of capacity coverage and availability. Wireless access points may be deployed indoor or outdoor.

Security is a vital problem in the design of a WMN. The client should have end-point-to-end-point security assurance. However, being different from a wired and traditional wireless network, a WMN could easily comprise various types of attacks.

Multicast routing in Wireless Mesh Networks

Multicasting is the ability to transmit a single stream to multiple subscribers at the same time. Unlike conventional streaming, it does not need one stream per recipient. Instead, there is one stream on any one segment of the network on which there is a subscriber. It is the task of the routers to track subscriptions and to create copies only on needed basis. Unlike broadcasting, segments on which there are no subscribers do not receive the stream. Multicasting is an unreliable protocol, using UDP as its basis. It is possible to add reliability to it.

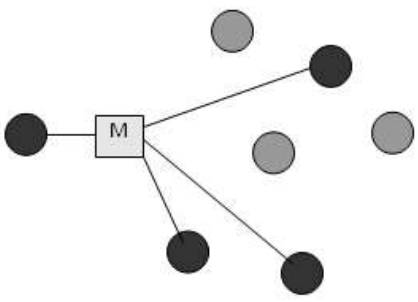

Fig.1: Multicast routing

Tele:

E-mail addresses: meena.dcn@gmail.com

Multicast is a form of communication that delivers information from a source to a set of destinations simultaneously in an efficient manner; the messages are delivered over each link of the network only once and duplicated only at branch points, where the links to the destinations split. Important applications of multicast include distribution of financial data, billing records, soft- ware, and newspapers; audio/video conferencing; distance education; and distributed interactive games.

Related Work

Some times, the high throughput protocols in multicast routing for wireless mesh networks relying on the assumption that the nodes behave correctly during metric computation and propagation. Hence these assumptions are vulnerable to attacks in [1] the ODMRP uses the rate guard techniques such as measurement based detection and accusation based reaction techniques.

Shared key distribution for all nodes may be impractical in such an adhoc network environment. An alternative solution to this key distribution is as in [2] S-ODMRP is proposed based on ODMRP and identity based cryptography, which secures the multicast routing and group key during the course of multicast routing discovery Secure routing of the mobile adhoc networks is the hard problem. For the above problem as in [3] optimized link state routing protocol with identity based cryptography is proposed.

The OLSR collects data about available networks and then calculate an optimized routing table. Identity based cryptography specifies a cryptosystem in which both public and private keys are based on the identities of users. This system has the property in which a user's public key is an easily calculated function of his identity, while a user's private key can be calculated for him by a trusted authority, called private key generator.

The field based routing uses less Information to route the packets in the network. Due to its characteristics, they are less expensive but such algorithms faces different type of security attacks.

For the above problem, in [9] a novel Enhanced Secure Field Based Routing (ESFBR) is proposed. The ESFBR is an extension to the existing secure field based routing algorithm. In which it identify and prevent the traffic flows from various attacks

The packets here transmitting are of geocasting type. I.e. they travel in a unicast manner from gate way to the group head and then the group head broadcast the message to all the members.

Proposed Solution

A reliable multicast protocol enables a process to multicast a message to a group of processes in a way that ensures all host destination group members receive the same message even if some group members are maliciously faulty. Reliable multicast has been shown to be useful for building multiparty cryptographic protocols and secure distributed services. Here, we present a high throughput reliable multicast protocol that tolerates the malicious behavior of unto less than one third of the group members.

In a typical high throughput multicast protocol, nodes periodically send probes to their neighbors to measure the quality of their adjacent links. During route discovery, a node estimates the cost of the path by combining its own measured metric of adjacent links with the path cost accumulated on the route discovery packet. The path with the best metric is then selected. High throughput protocols require the nodes to derive the path metric,thus relying on the assumption that nodes behave correctly during metric computation and propagation.

The block diagram for the reliable multicast routing is shown in Fig 2 in which the Secure-On Demand Multicast Routing Protocol (S-ODMRP) is implemented and trust model is computed by distributing trust keys to all the trusted nodes to provide security in the Wireless Mesh Networks which is vulnerable to attacks.

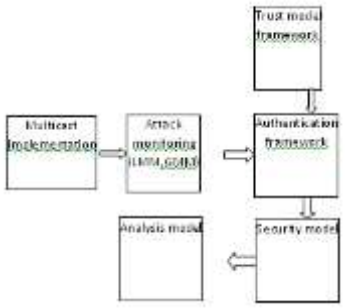

Fig 2: Block diagram for reliable multicast routing

Proposed methodology

The proposal achieves the data confidentiality, the data integrity and the source authentication simultaneously by the following three novel methods

- Local traffic is broadcasted ,which reduces the communication cost
- The self-healing mechanism cures the link failure caused by the failed routers and reconstructs the multicast key path
- The trusted key is distributed for secure multicast routing in the wireless mesh networks

The proposal has advantages with regard to the storage overheads, the computational delay and the approach to defend against the identified attacks.

The proposal uses the self healing mechanism in which the path is selected on the link basis in case of link failure which reduces the communication cost. And the trust key computing model is incorporated which can be used to choose the best path and ensure the reliability of the path by calculating the trust value of the neighbor nodes.

A member with good manners, such as normal joining or leaving of a group, enough residual power, and enough bandwidth, will obtain a high TV. And the secured high throughput multicast routing is achieved through the efficient trust key distribution to all the nodes in the network which is based on the trust value.

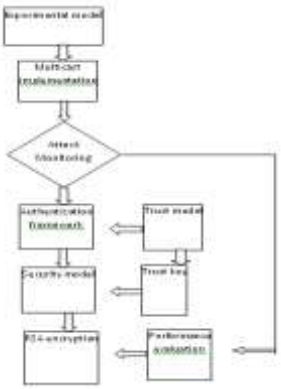

Fig.3: Multicast Data flow diagram

The above data flow diagram in Fig.3 shows the flow of proposed novel methods for reliable multicast routing in wireless mesh networks. At first architecture of wireless mesh

networks is created in the experimental model. And then a reactive On-Demand Multicast Routing (ODMRP) is implemented in the above architecture in which the data is delivered from the source. If no attacks occur in the delivery of data then the performance is directly evaluated at the destination.

Algorithm:

Algorithm for transformation node in Sending Side :

```
1. Void ack_received (char *buffer){
2. int num_pkts_to_send;
3. if(num_pkts_in_flight == 0) return;
4. num_pkts_in_flight--;
5. num_pkts_sent++;
6. If (latest_send_reqeust _seq<q.seq) then
7. check(q.from,q.sig)
8. latest_sending_requst_seq = q.seq
9. best_route=0
10. best_uplink = invalid node
11. check other node
12. fastest_uplink=q.from
13. get_new_query=True
14. send_queries.insert (q)
15.if(accusation_list.contains_accused_node(q.form))then
16. q.path_metric=0
17. else
18. q.path_metric=q.path metric*link metric(q.from)
19. if(get_new_query or route> best_route)then
20. best_uplink=q.from;best_route
21. best uplink=q.from;best_metric=q.path_metric;
22. q.from=node.id
23. if(get_new_query and is_receiver)then
24. start_time(reply_timeout)
25. sign(q);Broadcast(q)
26. if (ecn bit is zero, send two)
27. //packets in response else send none
28. if (ecn_bit == 0)
29. num_pkts_to_send = 2;
30. else
31. num_pkts_to_send = 0;
32. if(num_pkts_to_send > 0)
33. send_pkts ();
```

In case of attacks is identified in the delivery of data from the source to the destination , the self healing process is provided to cure from the link failure and trust key is provided to all the nodes in the network for the security of the data that ensures the reliability of the wireless mesh networks.

And the trust key distribution involves in the initial RSA encryption and all the trust nodes just forwards the packets instead of decrypting and re-encrypting in each and every intermediate node], thus it reduces the complexity of cryptographic key approaches and then the performance is evaluated.

Attack Reaction and Receiver Side:

```
1.void pkt_received(char *buffer)
2.int ecn_bit = ((packet *)buffer)->ecn_bit;
3.packet *ack_buffer;
4.num_pkts_rcvd++;
5.ack_buffer = create_ack(buffer
6.if(is_reciver)then
7.create salvage message
8. send_message( fastest_uplink)
9.If(accusation_list.contains_accuser_node(node_id)) then
10.return
11.create accusation message acc
12.acc.accused=best uplink
13.acc.accustion_time=(ePDR-pPDR)
14.accusation_list.add(acc)
15.create recovery message rr
16.rr.accusation=acc
17.Sign(rr)
18.if the ecnbit is non-zero,
19.set it in the ack header
20.if (ecn_bit != 0)
21.{
22.ack_buffer->ecn_bit = ecn_bit;
23.}
24.send the ACK to the sender
25.send_ack(ack_buffer,
26.((packet *)buffer)->src);
27.}
```

Results And Discussion

The On Demand Multicast Routing Protocol (ODMRP) is implemented in NS2. The performance of the proposed scheme is evaluated in terms of no of signatures, latency,bytes send per byte delivered and packet delivery ratio.

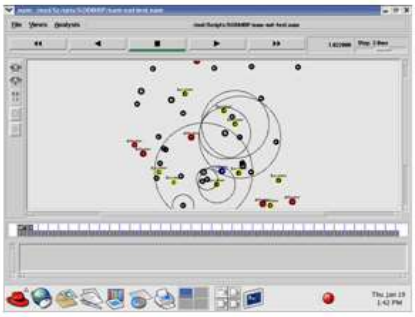

Fig.4: S-ODMRP implementation

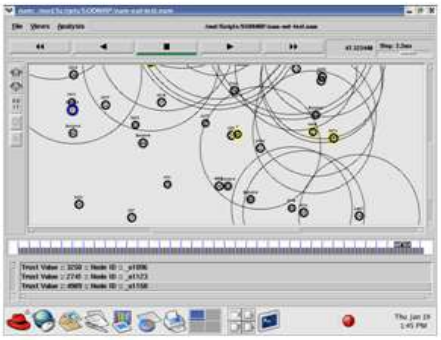

Fig.5: Isolation of attacker nodes

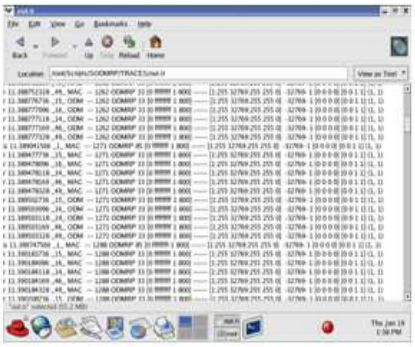

Fig.6: Trace file

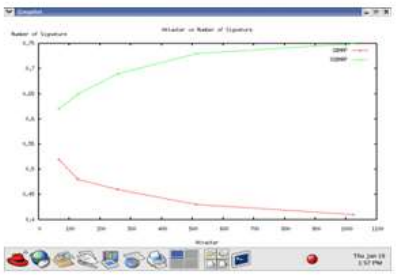

Fig.7: **Attackers Vs Number of signatures**

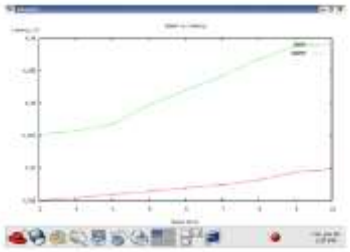

Fig.8: **Speed Vs latency**

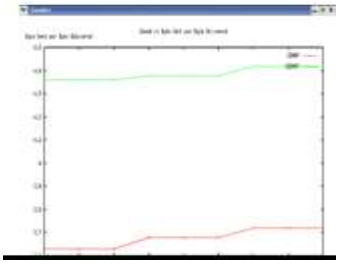

Fig.9**: Speed Vs Byte sent per byte delivered**

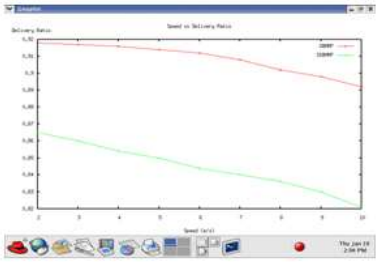

Fig.10: Speed Vs delivery ratio

In the simulation,a network of 50 mobile hosts placed randomly within a 1000*1000*m*2 areas. Radio propagation range for each node was 250 meters and channel capacity was 2Mbit/sec. Each simulation runs for 50 seconds of simulation time. The MAC protocol used in our simulations is IEEE 802.11. We used Constant Bit Rate as our traffic.

The size of data payload was 512 bytes. The nodes are placed randomly within this region. The multicast sources are selected from all 50 nodes randomly and most of them act as receivers at the same time. The data transmission takes place at 1st second as in fig.4 .The mobility model used is random way point, in which each node independently picks a random destination and speed from an interval (*min*, *max*) and moves toward the chosen destination at this speed. Once it reaches the destination, it pauses for *pause* number of seconds and repeats the process. Our *min* speed is 1 m/s, *max* speed is 20 m/s and *pause* interval is 0 seconds. .the malicious node are converted into isolated nodes at 2nd second as in fig.5 . Hence the ODMRP is vulnerable to attacks, the S-ODMRP is implemented and the trust value is provided to each node other than the isolated node based on the node id , so that it may improve the performance comparing to the ODMRP.

Conclusion And Future Work

Security is one of the major issues in the wireless mesh network. So Secure On-Demand Multicast Routing Protocol (S-ODMRP) is presented in a reactive security approach. Compared to existing routing protocols, the new proposal has several improvements in security of the wireless mesh networks which creates routes on demand and ensures the delivery of data from the source to the destination. Since the S-ODMRP applies "on-demand" routing technique, it avoids the channel overhead and improves the scalability. The NS-2 simulation results show the implementation of S-ODMRP and the trust key generation in the wireless mesh networks and also the improvement of performance with respect of number of signatures, latency, byte sent per byte delivered, delivery ratio. And the future work deals with the hash function of 1024-bit trust key generatied, RSA encryption and the performance analysis of modified S-ODMRP with S-ODMRP and ODMRP.

References

[1] R. Curtmola, J. Dong, and C. Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks", *IEEE Transactions on Mobile computing*, May 2011, PP. No.653-668 ,vol.10,issue:5

[2] Lei sun,Zishang dai, "Secure Multicast Communications in Mobile Adhoc Networks", *Journal on Mobile networks and applications 2008*,PP. No 616-620 ,vol.1

[3] AkshaiAgarwal,HuapengWu, Shushan Zhao, Shuping Liu, "A Secure Routing Protocol in Proactive Security Approach for Mobile Ad-hoc Networks", *IEEE Transactions on Mobile Computing 2008*,PP. No 2627-2632

[4] Dr.G. Padmavathi, D.Suganya Devi, "Performance Efficient EMOCT Algorithm for Secure Multicast Key Distribution for Mobile Ad-hoc Networks", *IEEE Transactions on* Wireless Communications and Mobile Computing 2009, *PP. No.*934-938

[5]Hyunsoo Yoon, Junbeom Hur, Seungjae Shin, "Bandwidth Efficient Key Distribution for Secure Multicast in Dynamic Wireless Mesh Networks", Journal of Computer Science and Technology 2009

[6] Feng He, Kuan Ho, "S-MAODV: A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol", *IEEE Transactions on Mobile Computing 2010,* PP. No.434-438

[7] Junbeom Hur, Youngjoo shin, Hyunsoo yoon , "DecentralizedGroup Key Management for Dynamic networks using proxy cryptography", *Mobile networks and applications 2007 , PP. No.*123-129

[8] Yong,Pei Qinqi , Ma Jianfeng, and Dong Lihua, "Efficient Secure Multicast Route using Genetic Algorithms for Wireless Sensor and Actor Networks", Wireless Network (WINET) Journal *2010*, PP. No.676-678

[9] Fahad T.Bin Muhaya, Fazal-e-Hadi and Atif Naser, "ESFBR Enhanced Secure Field Based Routing in Wireless Mesh Networks", *Indian Journal of Science and Technology*, PP. No.613-617

[10] S. Roy, V. G. Addada, S. Setia, and S. Jajodia, "Securing MAODV: Attacks and countermeasures," in Proc. of SECON '05. IEEE, 2005.

[11]R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in Proc. of IEEE SECON '07, June 2007.

[12] R. Draves, J. Padhye, and B. Zill, "Comparison of routing metrics for static multi-hop wireless networks," in Proc. of SIGCOMM '04, 2004.

[13] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," Elsevier Ad Hoc Networks, 2007.
[14] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in Proc. of IPSN '04. New York, NY, USA: ACM Press, 2004, pp. 259–268.
[15] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proc. SecureComm, 2006.