ISSN 2047-3338

Security Issues and Contradict Measures in Wireless Mesh Networks

Shabana Mustafa[1], Ali Raza[2] and Raeesa Qadeer[3]

[1,2,3]Department of Computer Science and Engineering, University of Engineering & Technology, Lahore, Pakistan
[1]shabana.mustafa153@gmail.com, [2]aliraza152@gmail.com, [3]aries_rathegr8@hotmail.com

Abstract—**As wireless networks have evolved into next generations, Wireless Mesh Networks (WMNs) have proved to be a massive infrastructure for better communication between enormous entity nodes. WMNs are extremely dependable, as every node is associated with all others likewise sketched in mesh layout. WMN network nodes consist of clients and routers, whereverthese play responsibilities as both routers and hosts.These mesh nodes transmit packets ahead as for theothers, this direct transmission is carried out up to the range of their destinations. Due to wireless associations in WMNs, there occur more chances of active and passive attacks to hit the mesh infrastructure. Apart from such hits, the distortion in messages is also prone to WMNs. There is a probability that a nodecan conciliate, when the system becomes prone to malicious attacks cause severe harm to networks. WMNs might tend to bevibrantfor the reason that regular changes can be made in both the mesh layout and the noderelationships. Major security challenges to WMNs are typically the same as challenges faced by all other networks; containing availability, confidentiality, authenticity and integrity. This paper includes the WMN security challenges, issues and the looms on hand to secure data communication between mesh nodes.**

Index Terms— **Wireless Mesh Networks, Mesh Router, Fairness of Network, Denial of Service, Compromising Nodes and Routing Protocol**

I. INTRODUCTION

WIRELESS Mesh Networks (WMNs), a promising technology, have brought the dream of the effortlessly connected world into realism. The networks can, with no trouble, efficiently establish connectionsto various intact cities using reasonably priced, offered wireless machinery. A amout of wired associated points is reliable to all customary networks or unwired hotspots that establish bonding between users. Inside a WMN system architecture, there connect a dozens or at least hundreds of unwired mesh nodes with WMN connection, and these hotspots communicate with each other so that the network waves can be dispersed in a huge region easily.

Mesh networking technology authorizes lot of major mobile networks in the globe. The technology influences established routing procedures initially developed for battleground connections by the services. The surplus temperament of mesh networks is a necessary feature required out for military strategy makers. By approaching aptitude and thorough decision making regarding the mesh network edges, highest performance and measurable broadband set of connections can be constructed at extremely low price by means of a mesh network.

This paper describes information about wireless mesh networks, consider the characteristics and node-to-node architecture of this network system. Starting from Section II, the basic structure of WMNs is drawn to simplify its meaning to the reader. In addition, major characteristics of WMNs with respect to different constraints like processor, mobility and bandwidth are described.

Furthermore, wireless mesh systems also face different challenges in maintaining security in Section IV. These may include active and passive attacks, or message distortion between nodes. Moreover, the security of adequate sharing between different nodes in mesh network faces little problems as these are the security requirements of all networks as well as quoted in Section V. For winding the paper up, Section VI containsprimary attacks on security norms of mesh networking between sources. Need to remind is the description of countermeasures to be taken for overcoming security attacks in mesh networks described at the end of this paper in Section VII. The last Section VIII concludes the paper, the idea of mesh networks and their standing in the telecommunication era in future concerns.

II. THE STRUCTURE AND CHARACTERISTICS OF WIRELESS MESH NETWORKS

A) Structure of WMN

The typical structure of WMN consists of Wireless Access Point (AP), Mesh Router (MR), Mesh Clients (MCs). Fig. 1 shows the structure of WMN.

The AP can connect multi MR. The main function of AP is to connect wireless network to the core network. Secondly, AP wants to connect wireless clients through MRs and make the end device equipped wireless network card use resources of core network through AP. APs of WMNs are costly as its provides many interfaces not only to attach with wireless networks but also wired networks.

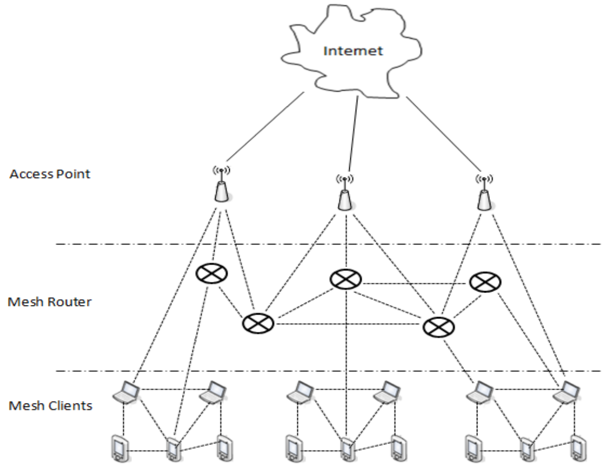

Fig. 1: Structure of WMN

The clients or mobile stations are connected to network through Mesh Routers (MRs). In WMNs, all information is transmitted by MRs from one client to another client. MRs have minimum mobility and ignorable battery restriction.

Mesh Clients (MCs) are the end devices that access the network.MCs are usually movable and its power is less. MCs canbe act as MRs and may not always be attached to the network.

B) Characteristics of Mesh Systems

The main characteristics of WMN are listed below:

- *Self-organizing and self configuring:* Addition or subtraction of nodes to network can be done easily after network establishing, to extend or narrowed network coverage.
- *The topology of WMN is very reliable*, for instance every node is attach to many other nodes. If a node is damage and disconnectof the network, the network can adapt itself to the change and can also rout a new path.
- *Multi-Hop:* WMN is a wireless multi-hop network. Every node can transmit and route packages to the other end point, and can select the best route from sender to destination. Nodes have functionality of repeaters to transferinformation from near nodes to nodes that are far enough.
- *Point-to-Point connection:* The connection between sender and destination can be directly, without pass through the centrenodes.
- *Scalability:* As the nodes in WMN increases ,the available bandwith also increased.

III. CONSTRAINTS

The constraints in WMNs are:

CPU: Processing power of the processor is limited, so massive processing at the nodes is slow.

Battery: Energy storage is less,for that reason nodes can not be used forbulkycomputations and transmission.

*Mobility***:** Convergence of the network is affected by mobility of MCs.

Bandwidth: Available frequency range among the MCs is limited.

IV. SECURITY CHALLENGES

Due to the unusual WMN constraints described above, the WMNs in front of challenges in attaining the network’s security. At first, the unlimited unwired channels have made WMN a way more prone to active and passive attacks. They have also tend to get affected by distortion in sent or received messages [1], [2]. The passive attacks have great influence on the mesh confidentiality, wheras the active attacks consequence in badly infringing the authenticaton, availability, non-repudation and integrity [2].

Second, the mesh routers are kept somewhere outside in the surroundings or buildingsfor robust communication. Therefore, node to be routed may be compromised because the physical defenseprovided to the routers is dreadfullyfrail. This would cause variousforms of malicious hits to the system not only from outside of the network, but inside the network.

Thirdly, the membership and topology of the WMN change frequently. This resemblance to the ad hocs can cause mistrust in the relationship, at any moment between the nodes.

Toconclude, due to scores of memory and calcuational constraints of WMNs, the complicated encryption algorithm cannot be implement, so the possibility of eavesdropped increased [3].

The thorough study of WMN’s specifics guide to the three serious security challenges faced by the mesh infrastructure [4]. These are:

- Detection of the damaged nodes
- Multi-hop routing
- Fairness in network

A) Detection of Damaged Nodes

For a WMN, it is a way more difficult to recognize the co-operative nodes connected within it. The physical protection of the nodes is essential. We describe four main attacks regarding the corrupt node detection. Main reason behind the definition of these attacks is the study of goals that the opposition wants to achieve.

The first simple attack relates to the substitution or the elimination of any intermediary node. To detect this type of hit, we need to obtain information of the defected node from its adjacent nodes when we observe a change in the network topology.

The second type can refer to a passive attack on the node. All the passive attacks use snooping or monitoring transmissiontechniques to get hold of information from the node [1]. The main thing that the adversary wantsis to obtain information that is being transmitted. Since the data is not altered, it is very difficult to detect passive attacks.

The third kind is about the internal status of the node in which the opponent tends to change the internal condition. The purpose of the opponent is to modify the routing algorithm, so that it finds easier to alter the network topology.

Toend with, the fourth attack comprises of the replication of a node and putting genetic copiesof the node somewhere in the deliberatelychosen locations in the WMN layout. This act allows the adversary to insert fake data and can also detach any segment of the WMN.

B) Multi-hop Routing

Here it is consider that the routing methodologies of the WMN ought to be guarded. The intruder is able to change networktopology by attacking the routing mechanism; therefore, entire WMN performance is affected.To change the routing mechanism, the opponent may interfere within the routing messages, alter the status of one or more network nodes, utilize the node replicas instead of the originals, or tend to execute Denial of Service attacks. The DoS attack is very dangerous as is simple to implementand difficult to prevent.

C) Fairness in Network

In WMN, the Mac layer should guarantee that no station is experiencing starvation of data transmission. Equitability in WMNs is identify with the right to gain entrance to the radio channel and access fortraffic sends through a given station.The steering or way choice protocolsare answerable for the honesty on the sent movement [5].The reasonableness issue in WMNs is cohorted to the amount of bounces between the hubs; this implies that if the rival increments the amount of jumps between a given sender and recipient hubs, it can diminish the transmission capacity being imparted [6].

V. SECURITY ISSUES

Security problems in WMNs are same as the requirements needed to secure traditional networks. These issues include:

- Availability
- Authentication
- Integrity
- Confidentiality
- Non-repudiation
- Authorization

A) Availability

Availability guarantees the survivability of system services disregarding denial of service (DoS) attacks. Availability does not strike a chord as a security concern as fast as do integrity and confidentiality. Yet the certification of availability is an imperative security issue. Denials of Service (DoS) attacks are frustrate for execution of WMNs. Truth be told, Dos is often a great approach of system services warfare. Also, the procedures needed to anticipate or moderate the impacts of misfortune of availability in light of the fact that the essential idea of availability guarantees that approved users have continuous access to the system services if there should be an occurrence of DoS strike. The availability in a WMN could be traded off by emulating ways.

1) Signal Jamming

An enemy can ambush on availability of the system by utilizing jamming to interface with correspondence on physical channel on the physical and Mac layers [7]. Standard protection instruments incorporates spread spectrum and frequency hopping, which make the enemy to enlarge the jamming go. One can likewise grumble the powers for jamming and get the aggressor capture.

2) Denial of Service (DoS)

A DoS attack might be started at any layer of WMN [7]. There are numerous methods for launching a DoS. A normal procedure is to flood the target framework with requests. The target framework comes to be so overwhelmed by the ask for that it couldn't process ordinary traffic. Firewall tenets could be changed in accordance with prevent ask for from a certain address. Be that as it may advanced attacks use "zombies" systems everywhere throughout the globe. This attack is known as distributed DoS [1] and it is incredibly difficult to avert. Intrusion detection and prevention framework are utilized to screen DoS attacks [8].

A DoS attack could be start either remotely or by a bargained hub in WMN. IDS/ IPS is troublesome to deploy in WMNs due computational and battery constraints.

3) Battery Exhaustion

Battery life is the most essential parameter for various nodes in a WMN. A Battery exhaustion attack generally called 'sleep deprivation attack' is a correct hazard and is a more stupendous number of dangerous than clear DoS attacks. Strike on CPU processing may avoid the availability from securing the service while battery exhaustion can deactivate the exploited person.

There are some battery administration and overseeing frameworks with the assistance of which one can make the appraisal of the measure of usable energy remaining just if such process does not devour excessively of the battery life itself.

B) Authentication

It empowers a node to guarantee the personality of the communicating node. Without authenticity, an adversary could imitate a node, subsequently picking up unauthorized access to confidential resources and meddling with the capacities of different nodes. With the usage of the thoughts, for example, omnipresent system, the more than enough networking nodes is sensible. All these nodes might as well have a genuine correspondence inside the system. The commonplace validation instruments include a brought together system which oversees confinement on the groundwork of capacity testaments. In a mesh system, the vicinity of such a concentrated system is some of the time not conceivable. Anyway there are a few courses as expressed underneath:

1) Secure Transient Association

The idea secure transient association is successful and straightforward [3]. Assuming that a user has a device, for example, widespread controller, then the user needs to be guaranty that it controls all and just her devices. That is, we have to association between the controller and devices. Right away this association needs to be secure; that is, there is no other user has the same controller.Thenthis association also needs to betransient. To ensure authenticity, this method can be employed in a WMN.

For the correspondence to other network, we can execute authentication methodology on the premise of open key cryptography, utilizing a node which has great computational force. The fundamental controller of the client can give authenticity for the sake of the node and inside the nearby network authenticity is given by secure transient association.

2) Imprinting

The methodology by which devices get the self-checked mediator's support is called imprinting. A framework node will recognize the first component as its holder that sends it a riddle key.

Demise is unavoidable for a network node. Possibly there is a time-out for getting another mystery key, or it is an issue in the network or in the node itself. The third reason may be that the possessor node demands the tyke node to end up dead and reborn. The time-out expiration give insurance from adversary that is, regardless of the fact that a mystery key is stolen, it might be swapped after a while. Provided that a node is traded off and the possessor node comes to think about it then holder node can ask the tyke node to bit the dust. At whatever point, a node bites the dust and reborn, it generally has a striking resemblance path, as it did the first time.

In a WMN system, the kid nodes might be the portable clients, PDAs, apparatuses and the possessor nodes could be the principle access point.

C) Integrity

The idea of integrity insurances that the data exchange from sender to receiver is saved sound throughout the entire communication process. Integrity guarantees that the data is not adjusted either deliberately or unintentionally throughout transmission. The purposeful modification of data is carried out by attacker and unintentional adjusting is typically because of transmission error. The normal approach to guarantee integrity of data is utilizing hash methods and message digestion [2]. Encryption is additionally use to protect integrity.

D) Confidentiality

It implies that sensitive data is just accessed and viewed by approved user. As it were, it ensures that sensitive data is never exposed to unapproved users. To administer the confidentiality of some delicate data, we have to keep them mystery from all questions that don't have the privilege to enter them. The data might hold sensitive data, for example, trade mysteries for commercial business, private medical or monetary records, or strategic military information, require confidentiality. Presenting such data to foes could expedite genuine suggestions.

For confidentiality, authenticity needs to be utilize first .It is vain to attempt to secure the mystery of a communication without first guaranteeing that one is conversing with the right one. When, authenticity is accomplish, confidentiality is utilized by encryption.

E) Non-repudiation

Non-repudiation ensures that the sender and the receiver of a message can't discredit that they have ever sent or appropriated such a message. It is useful for discovery and seclusion of a bargained node. For instance, when node-X appropriates a discourteous message from node-Y, non-repudiation permits node-X to denunciate node-Y utilizing this message and to guarantee different nodes that node-Y is bargained.

F) Authorization

Authorization is a procedure in which an entity is issued an accreditation by the trusted authentication authority. It is generally use to give distinctive access rights to diverse level users [9].

For example, we may need to make guarantee that network administration capacity is just accessible by the network administrator. Thus, there ought to be an authorization transform after the network administrator accesses the network administration capacities.

VI. SECURITY ATTACKS

In this area, the chief attacks that encroach the security criteria are inspected, and these are normally regarded as security attacks. There are ample kinds of attacks in WMN framework. The first sorts of these security attacks are portrayed in a couple of expressions as takes after:

A) Routing attack

The routing attacks in WMNs could be of the following sorts:

1) Byzantineattack

In this threat, the presence of originally cooperated nodes and their respective routing are not detected. This is because of malicious nodes that start the network through unacceptable operations, hence affecting the network routing. This network operation seems to be normal for other nodes as well; therefore in the end, the attack results in brutal consequences to the entire network.

2) Location disclosure attack

These attacks unveil a little about the structuring of the network or the position of nodes, for example, which different nodes are neighbouring to the aim, or the physical region of a node.

3) Routing table overflow attack

In this attack, an attacker plan to makes enough routes to the nodes that don't exist. This is carried out with a specific end goal to put off new unique routes from being made and subsequently the generally speaking protocol execution gets overpowered. This attack may additionally escort to the Denial of Service or the resource exhaustion dangers. The Denial of Service attack is portrayed further.

B) Sinkhole/ black hole attack

In this attack, there comes a malicious node that interfere with a node by sending a data packet and promotes itself to it. For this, the malicious node uncovers the briefest way to the node, consequently utilizes a routing protocol to publicize itself.

C) Wormhole attack

The attacker acknowledges packets at one position in the network and channels them by decision to one more area in the network. After that, the packets are re-broadcasted into the network, and the channel between two planned intruders is said to be the wormhole [19].

D) Denial of Service attack

Because of a few malicious activities in the system or any sort of unintentional breakdown, denial of service attack runs across the network system. This attack is made by flooding the concentrated source in such a foreseeable path, to the point that it quits running or no sooner initiates rightly [17]. An alternate manifestation of the DoS attack is the distributed DoS attack (DDoS) which is alluded to as more extreme than DoS to the remote network networks. There are some traded off nodes which have a tendency to contrive together and influence the network security gravely. Such nodes are a part of the network and cause the DDoS attack to start. The DDoS attack additionally instantiates SYN flooding.

E) Impersonation attack

Because of this risk, there emerge genuine security hazards in WMNs. In the event that any fitting authentication of every node is not conveyed, then it is prone to have helpful nodes to join with the network, cheating other trustful nodes and sending wrong routing data [20]. This figures a bargained node to get contact to the network administration framework and it speaks to itself a legal user who has interesting benefits to modify the configuration of the system.

Security measures for this sort of attacks could be to have solid authentication strategies that are pertinent in setting where a cluster of node needs to believe the source node from which it has accepted and archived the data.

Hence, it is accepted that the routing apparatus of WMNs must be ensured. The normal system, to certification integrity of data, is utilizing hash methods and message absorbs.

VII. SECURITY MEASURES FOR WIRELESS MESH NETWORKS

The point when keeping tabs on security measures for WMNs, different routing protocols are petitioned they are convenient in checking the finish of security methods and their productivity. Similarly as with the course of time, the routine routing protocols don't perform better and underpin the WMNs in view of their evolutionary topologies and transportability of nodes.

As time evolved, diverse routing protocols have developed in perspective of the portability of nodes and self-arranged conduct of WMNs. However these protocols did not turn out to be material for security methodologies. Subsequently, there excited uncompromising issues in the support of wireless mesh systems security.

Moreover, various Secure routing protocols have seemed to subsistence. Some dissimilar ones are portrayed underneath:

A) Authenticated Routing [12], [18]

Authenticating routing protocol is suitable to the routing protocols that are actualized on requests. This protocol confirms the routing data through publicized key certificate and a dependable CA. For this reason, some essential conditions of such protocol lie here. There must be a trusted certificate server is alluring. This server is to allocate and handle the certificates. The server achieves for an open key certificate to each node before joining the network.

B) Demand Routing Protocol [11]

In this protocol, the TESLA technology on the groundwork of DSR is accentuated. TESLA is a transmit mechanism for check that confirms every package by the utilization of a messenger authentication code i.e. MAC. It additionally avoids the nodes from having false MACs. This is done by swapping the postponed keys and using time synchronization. The essential approach behind this protocol is that firstly, the sender is to send the messenger on top of its MAC, then a key that checks the MAC. The point when the receiver gains the messenger, it store it utilizing that MAC, and the confirmation of the messenger is completed by utilized the separate key.

To make sure the arrangement of MAC and the separate key, there is a need of time synchronization. The essential conditions of the demand routing protocol identify that the sending and the accepting nodes have a key which is imparted. Every node in the network obtains the preparatory check esteem of additional nodes and their separate clocks must be harshly synchronized.

C) Secure Ad Hoc On Demand Distance Vector [14],[15]

This is a safe routing protocol dependent upon Ad Hoc on Demand Distance Vector. Its essential condition is to transmit the general population keys to each node for imprint. It possesses two systems to certification the security on Ad Hoc on demand distance vector. One is the computerized imprint which guarantees the unwavering quality of data in the packet that does not oblige its alteration while sending packets between nodes. The other technique is the restricted hash chain that checks variable part of the packet like measure of hops in the packet.

The preference of this protocol is to utilize double imprint system to solve the challenge of checking the reactions to the middle of the intermediate nodes' routing requests. The inconvenience of this protocol is that it uses asymmetric cryptography for its reason to be carried out. This system utilizes a pack of assets on middle of the intermediate nodes, so it is costly.

D) Secure Efficient Distance Vector Routing [13]

This is a safe routing protocol that grows from Destination Distance Sequence Vector whose focal thought is to utilize the hash chain components to check the sequence number and amount of hops in routing updating packet. Since the restricted hash chain trademark could evade an invader from misrepresenting a sequence number greater than the real one or expressing a more diminutive amount of hops than the substantial ones. The point when gain a updated routing packet, at the outset, a node makes utilization of its hash value for the check of the packet, if the confirmation is endorsed, it then changes its track table values, or else it rejects this packet.

The preference of this strategy is the variety of the one-way hash chain for the verification of the validation which basically decreases the figuring trouble. The disadvantage of this system is that a dependence entity is needed in the network to allocate and keep up the confirmed node's component since the verification hash chain component is disconnected by a trusted entity. This is prone to cause single-focus breakdown. In the event that the solid entity is chipped in, the complete network will break down.

E) Secure Link State Routing [16]

This is a protected protocol which is dependent upon connection conditions and protects the routing protocol by method of connection states like Zone Routing Protocols. This protocol has an essential condition that every node has several open & private keys and nodes additionally have open keys transmitted to different nodes.

The Secure Link State Routing has two strategies. The leading is, it could stop IP address tempering in networks; the second is, it may record the packet transfer frequency of neighbours and assuming that it surpasses the given value, this neighbouring node is then private as an invader and at last, its packets are no more improved. This could bind to the Dos attack like the flooding in an extremely little territory.

The benefit of this practice is utilizing the method of viewing the neighbours to thwart the Dos attack. The hindrance is that it utilizes unbalanced cryptography which devours an unlimited extend of resources on halfway nodes.

F) Secure Routing Protocol [10]

This protocol expands subsisting on-interest routing protocols with the ability of distinguishing and clearing fake routing data and subsequently kills from tempering attacks, replaying and adulterated routing. This Protocol determines getting accurate data about topologies. It has an essential condition that the sender and the receiver nodes hold keys that are imparted for confirmation and correspondence throughout packet exchange.

VIII. CONCLUSION

At a mechanical level, present WMNs are far off from being capable, and protocols whatever statures must be broadened to supply transporter evaluated services that allow internet service providers to produce incomes from mesh networks and accordingly reward for the trusts of the mesh base. Next, concerning the security, mesh systems are a way more undeveloped than the wired networks. However, without considering the wired medium, extra protection is sought to insurance a secured data transmit. Taking everything into account, the principal indicate contemplate in security is to shield the user privacy. The area of a user can smoothly be persistent by the mesh node joined with the user. It is very little clear that if and how this privacy is satisfactorily secured. In this manner, the chances are far above the ground and the tests are more challenging to react. Yet, on account of the issues, a conflict is raised that WMNs still maintain a massive research impending that values advancing, basically utilizing experimental evaluations over real testing.

REFERENCES

[1] S. Hansman and R. Hunt, “A Taxonomy of Networkand Computer Attacks”, June 2004.

[2] W. Stallings, “Network Security Essentials”, Third Edition, Prentice Hall, July 2006.

[3] N. B. Salem, J. P.Hubaux, “Securing wireless mesh networks,” IEEE Wireless Communication, February 2006.

[4] I. F. Akyildiz, X. Wang and W. Wang, "Wireless Mesh Network: A Survey", in Computer Networks and ISDN Systems, December 2004.

[5] S. Glass, M. Portmann, and V. Muthukkumarasamy, “Securing Wireless Mesh Networks”, IEEE Internet Computing, Vol. 12, 2008.

[6] N. B. Salem and J.-P.Hubaux. “A Fair Scheduling for Wireless Mesh Networks”, in proceedings of WiMesh, September 2005.

[7] X. Gu and R. Hunt, “Wireless LAN Attacks and Vulnerabilities”, in the proceeding of IASTED Networks and Communication Systems, 25-29 April, 2007, Thailand.

[8] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks" in Kluwer Wireless Networks Journal , Vol. 9, No. 4, September 2003.

[9] R. Malik, M. Mittal, I. Batra, and C. Kiran, “Wireless Mesh Networks (WMN)”, International Journal of Computer Applications, Vol 1, No. 23, 2010.

[10] P. Papadimitratos, Z.Haas, “Secure routing for mobile ad hoc networks”, in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 31,2002.

[11] Y. C. Hu, A. Perrig, D. B. Johnson, “Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks”, in Proceedings of the MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA.

[12] A.Perrig, R.Canetti, D.Song, J.D.Tygar, “Efficient and secure source authentication for multicast”, in Proceedings of

Network and Distributed System Security symposium, February 2001, pp35-46.

[13] Y. C. Hu, D. B. Johnson, and A.Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[14] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing”, ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106-107, July 2002.

[15] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols”, in Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pages 1-10. September 2002.

[16] P. Papadimitratos and Z.J. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks”, IEEE Workshop on Security and Assurance in Ad hoc Networks, January 28, 2003,Orlando, FL.

[17] R. P. Karrer, A. Pescapé, T. Huehn, “Challenges in Second-Generation Wireless Mesh Networks”, EURASIP Journal on Wireless Communications and Networking 2008, September 2008,Germany.

[18] L. Li, Y. Jiankang, H. Jinghe, “Research on the Security Issues and CounterMeasures of Wireless Mesh Network”, China Ship Research and Development Academy Beijing, China, September 2012.

[19] P. Yi, T. Tong, N. Liu, Y. Wu, J. Ma, “Security in Wireless Mesh Networks: Challenges and Solutions”, Sixth International Conference on Information Technology, April 2009.

[20] H. Redwan, K. H. Kim, “Survey of Security Requirements, Attacks andNetwork Integration in Wireless Mesh Networks”, Japan-China Joint Workshop on Frontier of Computer Science and Technology, December 2008.