International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

Protection during Wireless Mesh Network Challenges and Solutions

Dr. A. S. Shanthi[1], G. Kokila[2], K.Deepa[3]
[1,2,3] *Department of Computer Science and Engineering, Tamilnadu College of Engineering, Tamilnadu, India.*

Submitted: 01-11-2022 Accepted: 12-11-2022

ABSTRACT:
Wireless Mesh network (WMN) is a hopeful technology that has grown in popularity in recent years. WMN has the feather of self-organization, distributed organization. The main topological characteristic of WMN is that there is only one or some nodes connecting to the infrastructure network as a gateway, and all other nodes connect to the gateway through the relay of the neighboring nodes, and then connect with the internet. In this paper, we discuss some of the routing protocols, OLSR, an Optimized Link State Routing Protocol, and FSR, Fish Eye State Routing Protocol, in detail and present various ad hoc routing protocols and their properties. Because of the nature of wireless and multi-hop networks, security flaws have become critical issues. Therefore, a specified security mechanism should be introduced. The research on the key security theories and detection of intrusion of WMN has become of great significance both theoretically and empirically. This object starts with the introduction of the basic organization and characteristics of WMN, presents major security problems and key security approach gradually to the reader, and concludes with the comparison of several secure routing protocols.
Keyword: Wireless Mesh Networks, Self-organization, Mesh, Ad Hoc networks, OLSR, FSR.

I. INTRODUCTION

Wireless Mesh Network (WMN) is an emerging technology and has been developing rapidly in recent years, which represents a whole new network concept. Because of the nature of wireless and multi-hop networks, security vulnerabilities have become crucial problems. We first introduce the basic association and characteristics of WMN, then present major security problems and key security approaches to advance the reader gradually. Wireless Mesh Networks are dynamically self-organized networks that employ multi-hop communications to transmit data traffic to and from Internet entry points. WMNs are comprised of three types of nodes: access points, mesh routers, and mesh clients. Access points are special routers with a high-bandwidth wired connection to the Internet, and they serve as interfaces for WMNs. The ultimate users in WMNs are mesh clients, which can be desktop computers, laptops, PDAs, or cellular phones. Most mesh clients run on batteries and only have a limited radio transmission range. For mesh routers, they provide multi-hop connectivity between mesh clients and access points. Mesh routers have power supplies and minimal mobility. In addition to mesh networking among WMNs, the gateway/bridge functions in mesh routers enable the integration of WMNs with various other networks. The network of mesh routers and access points creates a wireless backhaul communication system, which provides each mesh client with a low-cost, high-bandwidth, and seamless multi-hop connection to the Internet. Despite recent advances in research and development in WMNs, many challenging problems still remain. In the end, we conclude with a comparison of several secure routing protocols.

1.1 Conceptions

The Wireless Mesh Network, or WMN, is a dynamically self-organizing and self-configuring network that automatically sets up a Mobile Ad Hoc Network (MANET) for its internal nodes to obtain the connectivity of nodes. The Wireless Mesh Network (WMN) is a hybrid network that combines WLAN and MANET, with backbone nodes connected in an ad hoc network and clients connecting to backbone nodes via WLAN. Many natural technologies developed for WLAN and MANET could be easily applied to WMN, which makes WMN more appealing. WMN combines the advantages of WLAN and MANET, providing a large-capacity, high-speed, and wide-covered network connection and is an ideal model to solve the last-mile problem in wireless network

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

distribution. WMN could be employed on various occasions, like cities, school campuses, emergency situations, and battlefields. MR provides strong switch ability, minimum mobility, and negligible battery restriction. Besides the traditional routing facilities like gateway and bridge, MR also supports routing functions specifically designed for WMN as the backbone of WMN. Meanwhile, MC could be designed with a light architecture that supports the most basic routing capabilities and communication protocols. Therefore, MC only needs one wireless interface to achieve its function.

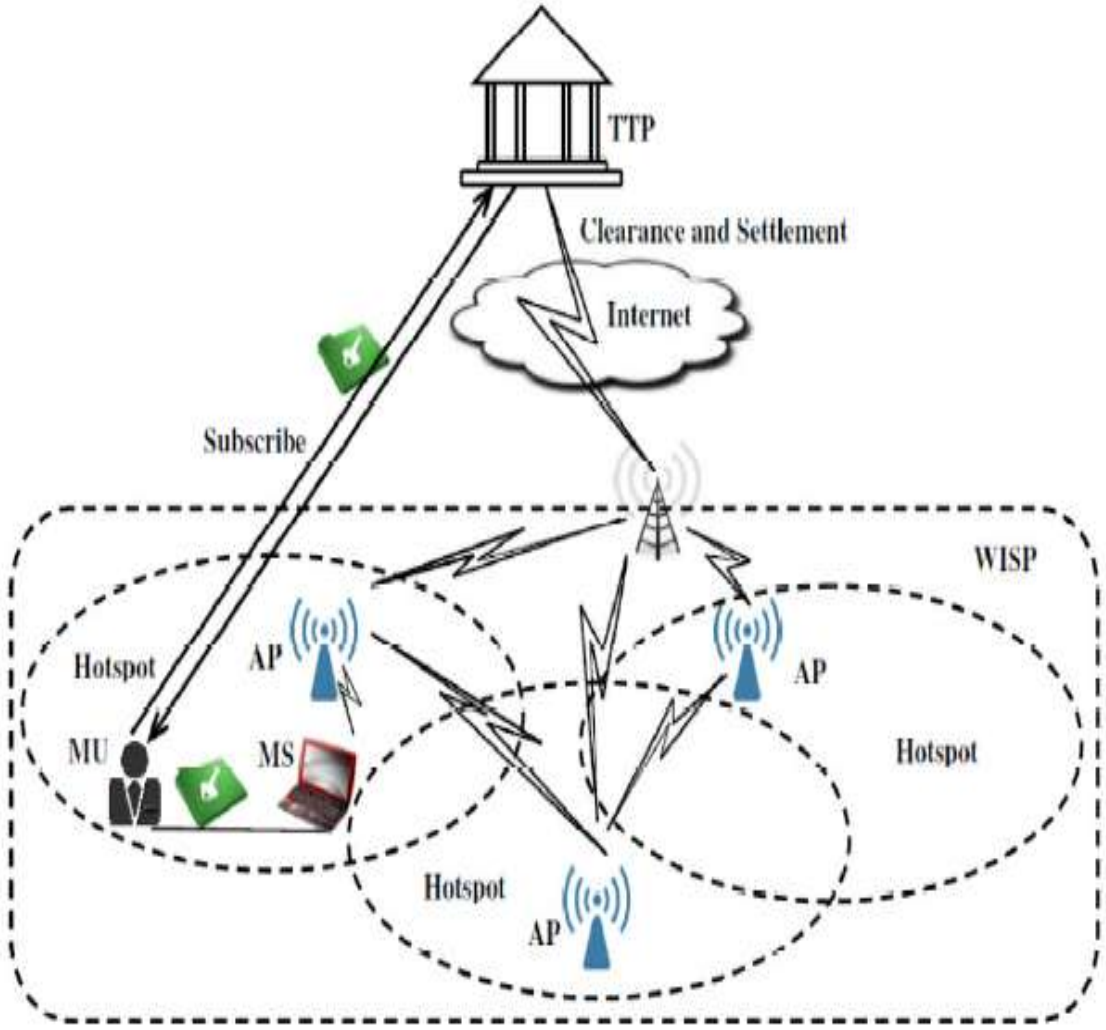

Fig 1. WMN architecture and different network entities in the local authentication protocol

1.2 The Characteristic of WMN

- WMN employs the Ad Hoc Network and hence has the abilities of self-initialization, self-reparation, and self-organization.
- WMN is a wireless multi-hop network based on the backbones as part of the wireless infrastructure.
- MR has a relatively fixed position, dedicated to maintaining the network and providing services to MC. Therefore, the existence of MR could largely alleviate the service load on MC.
- The mobility of terminals could be easily supported by the wireless infrastructure.
- MR integrates heterogeneous networks, including wired and wireless network, which enables WMN to support different network connections.
- The energy restriction on MR and MC is different.
- WMN is not stand-alone and should cooperate and be compatible with other types of wireless networks.

1.3 WMNs Must Capture The Following Features

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

- Many existing routing protocols use minimum hop as the performance metric to select the routing path, but this has been demonstrated to be inefficient in WMNs.
- Setting up and maintaining a route path in a WMN will take a long time due to the large size of a WMN network.
- It is critical to have a scalable routing protocol in WMNs.
- The routing protocol in WMNs must be robust to link failures or congestion.

1.4 Comparison for Types of Wireless Networks

The unique characteristics and the development trend of the future network highlight the WMN. Table 1 makes a comparison with WMN, Cellular networks, mobile ad hoc networks (MANET), WLAN, and Wireless Sensor Networks (WSN).

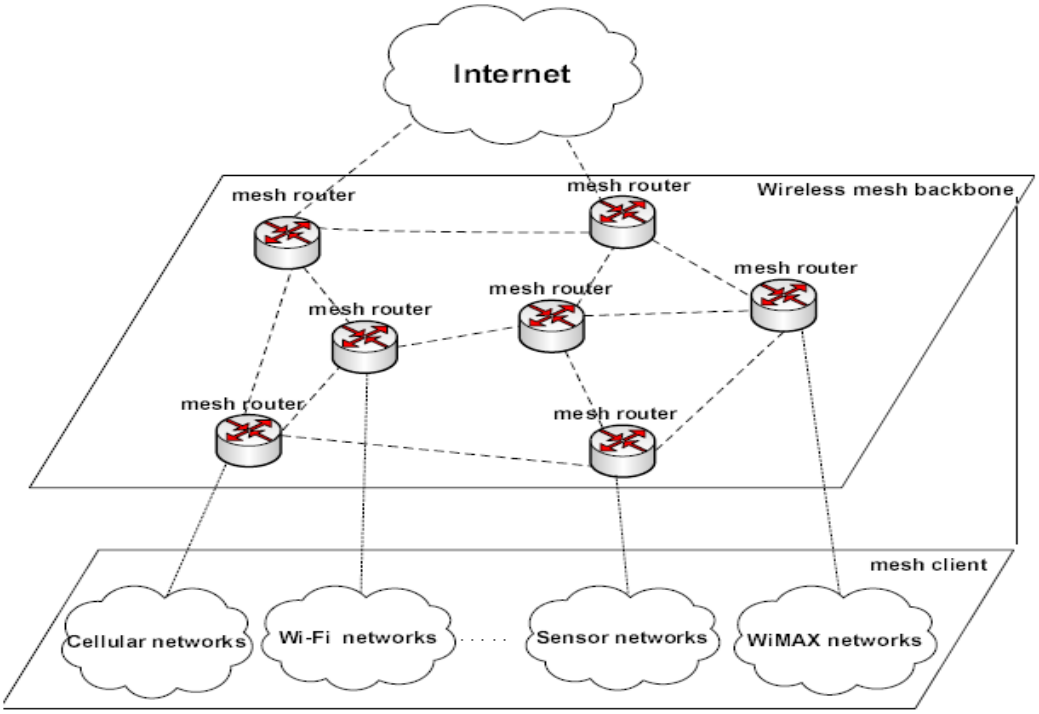

Fig 2. Different types of infrastructure of WMN

Table1 Comparison of different wireless networks

	WMN	**Cellular Network**	**MANET**	**WLAN**	**WSN**
Topology	NP to NP (Mesh)	P to NP	Dynamic Topology	P to P	Dynamic Topology
Cover Range	Metropolitan Area	large area via multi-cells	Usually Local Area	Local Area	Extreme Large
User Capacity	Large	Very Large	Relatively Small	Small	Extreme Large
Control Method	Distributed	Centralized	Distributed	Centralized	Distributed
Design	User Connection	User Connection and Communication	Communication	Communication	Data Transmission
Node Mobility	The Minimum mobility of	Stationary base stations with mobile clients	Dynamic topology of all nodes	Stationary Access Points	Dynamic topology of all nodes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

	the backbone network MR could be stationary or mobile. MC was free to move around.				
Energy Restriction	Varies according to different devices connected to the network	Clients need energy saving protocols	Clients need energy-saving protocols.	Clients need energy-saving protocols. Access points do not have restrictions.	Energy is a vital problem.

II. SECURITY PROBLEMS OF WMN

2.1 Problems in Security Aspect

Protection is a vital problem in the design of WMN. The client should have end-point-to-end-point security assurance. However, being different from traditional wired and wireless networks, WMN could easily be comprised of various types of attacks. Even the WMN infrastructure like MR could be relatively more easily reached and adapted by attackers. Therefore, appreciative security measures should be taken. Some common protection threats in WMN are listed below. The designer of the network should try to avoid these threats and maintain the reliability of WMN.

Physical Threat

Generally, routers in wired networks are properly protected. Therefore, an attack on the routers in a wired network is difficult. However, the routers are usually deployed outdoors, like on roofs of buildings or on street lamps. Therefore, physical protection for the routers of WMN is very weak. This would cause attacks on the routers like tempering the information in the router, stealing the private key for authentication stored in the router, or even replacing the router with a malicious one, and hence the attacker would be able to connect to the network as if he was a legal node and send incorrect routing information. Therefore, secure routing protocols are essential to fight against this kind of attack.

Multi-Hop Routing Problem

It is well known that wireless communication is vulnerable to passive attacks like interception and active attacks like packet tempering or DoS attacks. These inherent security problems will be addressed in WMN. In 802.11 WLAN, every node connects with the AP, so the management of nodes in WLAN is more viable than in multi-hop networks like WMN. If all security mechanisms are on the wireless gateway on one side of the WMN, there will be a huge delay in detection and response to the attack, which will bring benefit to the attacker. Besides, since the distance of the clients to the node with an Internet connection varies, nodes far away from the Internet connection might get very limited bandwidth, which provides vital reasons to design a proper protocol to ensure equity among the clients and protect the equity.

Confidentiality with Integrity

Keeping the information sent out by MR from being tempered or intercepted is very crucial in WMN. This could be realized by employing encryption in various layers. Hence, the foremost problem becomes finding a viable encryption policy for protecting confidentiality and integrity while minimize the algorithmic complexity and cost of management. The existing WEP is not suitable due to its inherent flaws.

Authentication in WMN

A strong authentication mechanism is necessary in order to prevent an unauthenticated node from connecting to the WMN. Every node that joins WMN should be able to verify the identities of others. In WMN, the lack of terminal facilities causes the necessity of a distributed Authentication mechanism to verify every MR or a national authentication mechanism by appointing one particular MR as the authentication server. In both cases, the authentication should be based on security associations outside IEEE 802.11.

Routing Security

By attacking the routing policy of WMN, an attacker could affect the performance of the network by altering the topological information in

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

the routing packet. There are various reasons behind the routing policy of WMN. An attacker could affect the performance of the network by altering the topological information in the routing packet. There are various reasons behind such an attack. For example, a reasonable attacker could monitor the communication by attracting data flows to pass a malicious MR by tempering the routing information, or the attacker could start a DoS attack so that all clients could not get what they needed.

The Following Measures to Attack the Routing Mechanism:

- ❖ Tempering the routing information
- ❖ Modifying the status of one or more MR,
- ❖ Start a DoS attack

Among them, the DoS attack is a simple yet effective attack on the routing mechanism. It is simple to implement and resistant to defense. DoS attacks performed by a single node could be prevented by monitoring each node's source frequency of sending route information and setting a valve at the frequency. However, attackers might also perform a distributed DoS or DDoS.

1.5 Possible Attack Types in WMN

Tempering:

Routing protocols in WMN assume that nodes in the network are cooperative, which would not modify any information irrelevant to itself while forwarding and hence do not check the integrity of the packet. This allows the attacker to easily temper any specific field in the packet, e.g., sequence number and number of hops in AODV or node sequences in DSR, and hence results in wrong routing decisions like redirection or route loops, which degrades the performance of the entire network. The fundamental reason for the attacker's ability to temper the routing information is the lack of integrity checks.

Pretending:

Because routing protocols cannot verify the source address, attackers could pose as legitimate nodes and join the network. Even worse, it could block the legal node, receiving and sending packets in the name of the legal node. The fundamental reason for the attacker's ability to pretend is the lack of source address verification.

Forging:

An attacker could forge and broadcast incorrect routing information, such as declaring a broken link or responding with a non-existent route. This might cause serious problems like loops, isolated networks, or nodes. The fundamental reason for the attacker's ability to forge is the lack of packet data verification.

Analysis of Topology and Data Flows:

Routing information exists in both the routing request packet and the data packet. For example, the data packet in DSR contains the information of nodes from the source to the destination. The attacker could obtain the topological information position and nearest situation of nodes by analyzing this information, and further analysis of the number of flows might even provide information about the function and role of the particular node. According to this information, an attacker could precisely locate the network control node or, in a situation like a battlefield, the commander.

Resource Depletion Attack:

An attacker could send a large number of useless packets like routing request packets or data packets, depleting the resources of the network and nodes, such as bandwidth, memory, CPU, or batteries.

Wormhole Attack:

Two distant points in the network are connected by a malicious connection using a direct low-latency link called the wormhole link. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the attacker captures wireless transmissions on one end, sends them through the wormhole link, and replays them on the other end.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

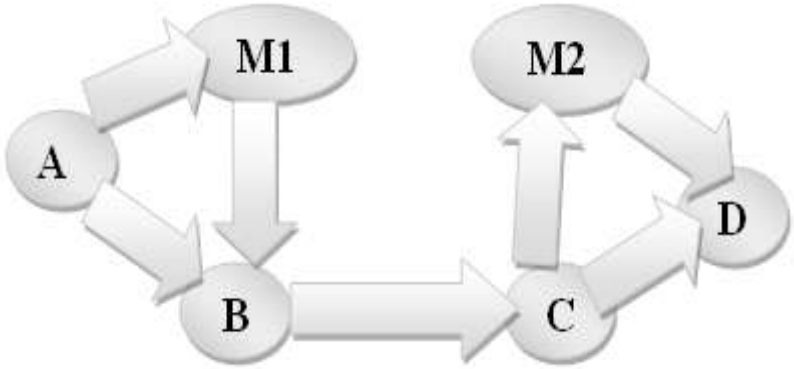

Fig 3. Illustration of Wormhole Attack

Figure 1 is a simple illustration of the wormhole attack. From node A to node D, the normal route should be A-B-C-D.

Blackhole Attack:

While receiving a routing request, the attacker claims that it has a link to the destination node even if it does not, and then forces the source to send the packet through it without forwarding the data packet to the next hop.

Rushing Attack:

In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time, keeping other nodes busy processing legal routing request packets.

III. SOLUTION TO SECURITY PROBLEMS ON ROUTING PROTOCOLS

The routing protocol is a vital part of WMN because it directly determines the implementation of network functions and their efficiency. Due to the special characteristics of WMN, such as the mobility of nodes and changeable topology, traditional routing protocols are not suitable for WMN. In recent years, various WMN routing protocols have emerged, and most of them have adopted the ideas of MANET routing protocols like DSR, AODV, and DSDV. However, although these protocols give full consideration to the mobility and self-organization characteristics of WMN, they failed to take security factors into account, which resulted in severe problems in security in WMN. In this case, many secure routing protocols have come into existence. Some typical ones are introduced below.

SRP Secure Routing Protocol

SRP adds the ability to identify and discard false routing information to existing on-demand routing protocols, thereby eliminating tampering, replaying, and forging routing attacks. SRP ensures acquiring correct topological information. The prerequisite condition of SRP is that the source and the destination nodes have a shared key for verification and communication.

ARAN Authenticated Routing for Ad Hoc Networks

ARAN is suitable for on-demand routing protocols. ARAN uses a public key certificate and a trusted CA to verify the routing information. The prerequisite conditions of ARAN are that a trusted certificate server is needed to distribute and manage the certificates and every node should obtain a public key certificate from the server prior to joining the network.

A Secure On Demand Routing Protocol for Ad Hoc Networks

A secure routing protocol using TESLA technology based on DSR TESLA is a broadcast verification mechanism that verifies the data packet by Messenger Authentication Code (MAC) and prevents the forging of MAC by employing time synchronization and delayed key exchanging. The basic process is that the source sends the messenger and MAC first, and then sends the key for the verification of the MAC. At the destination, the receiver stores the message first and then verifies it using the key. To ensure the order of MAC and key, time synchronization is needed. The prerequisite conditions are that the source and the destination nodes have a shared key; every node in the network possesses the initial verification value of other nodes; and their clocks must be approximately synchronized.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 317-325 www.ijaem.net ISSN: 2395-5252

SEAD Secure Efficient Distance Vector Routing for Mobile Ad Hoc Networks

SEAD is a secure routing protocol that extends from DSDV whose basic idea is to use the elements in the hash chain to verify the sequence number and number of hops in the routing update packet. Because of the one-way characteristic of a hash chain, this could prevent an attacker from forging a sequence number larger than the real one or declaring a smaller number of hops than the real one. When a node receives an update routing packet, it uses its hash value to verify the packet. If the verification is passed, it then modifies its route table, and else it discards this packet. The advantage of this method is the adaption of a one-way hash chain to verify the authentication, which largely reduces the computational complexity. The disadvantage of this method is that a trusted entity is needed in the network to distribute and maintain the verification element of every node because the verification element of a hash chain is detached by a trusted entity.

SAODV Secure Ad Hoc on Demand Distance Vector

SAODV is a secure routing protocol based on AODV. Its prerequisite condition is to dispatch the public keys to all nodes for signature. It employs two mechanisms to ensure security on AODV. One is the digital signature, which ensures the integrity of data in a packet that does not need to be modified while forwarding. The other one is the one-way hash chain to verify changeable parts like the number of hops in the packet. Its advantage is that it uses the double signature mechanism to solve the problem of verifying the answers to the routing requests of intermediate nodes. The disadvantage is that it uses asymmetric cryptography, which consumes a lot of resources on intermediate nodes.

SLSP Secure Link State Routing for Mobile Ad Hoc Networks

SLSP is a secure protocol based on link states and protects routing protocols using link states like ZRP. The prerequisite condition of this protocol is that every node has a pair of public and private keys and has a public key dispatched to other nodes. SLSP has two functions. For one thing, it could prevent IP address tampering; for another, it could record the packet-sending frequencies of neighbours and, if it exceeds a certain threshold, label this neighbour as an attacker and stop processing its packets. This could restrict DoS attacks like flooding to a very small area. The advantage of this algorithm is that it uses the mechanism of monitoring its neighbours to prevent DoS attacks. The disadvantage is that it uses asymmetric cryptography, which consumes a vast amount of resources on intermediate nodes. Table 2 gives a comparison of these secure routing protocols.

IV. CONCLUSION

In summary, WMN combines the existing WLAN and MANET technology with infrastructure, client, or hybrid modes to provide many new characteristics for the application. However, the design of WMN routing protocols encounters many problems, like mobility and security. Although many routing protocols from MANET could be applied to WMN and solve the problem of mobility, security problems are still crucial. Many secure routing protocols have been proposed recently. However, they all have pros and cons, which limit their application. Moreover, most secure protocols need shared-key dispatch or an existing PKI for all nodes in a WMN, which is not practical in WMN and might compromise the characteristics of self-initialization and self-organization. Therefore, how to find a proper way to solve these security problems would be an important topic for WMN.

Table 2 Comparison of Secure Routing Protocols.

Protocol Name	Suitable for	Prerequisite Conditions	Main Security Tech	Verification Part	Pros	Cons
SRP	DSR	Key shared between source node and destination node	Messenger authentication code	Source address, Destination address, Messenger ID	Simple algorithm, Wide application situations	Lack of protection for routing maintenance messenger, intermediate nodes cannot reply routing request

ARIADNE	DSR	Dispatch the TESLA verification key, key shared between source node and destination node, public key certificates	One-way hash chain Messenger authenticatio ncode	Whole packet, routing sequence	Use symmetric cryptography and TESLA technology, low computational complexity and Overhead of management	Need time synchronization, bandwidth wasted in sending keys, latency inverification
ARAN	AODV DSR	Establish a certificate server responsible for issuing and maintaining the public key certificate of every nodes	Digital signature	Whole packet	Ensures authentication, integrity and non-repudiation	High computational complexity, CA is needed, intermediate nodes cannot reply routing request
SEAD	DSDV	Dispatch verification initialization value	One-way hash chain	Sequence number, number of hops	Low complexity in computation	A trusted entity is needed to dispatch and maintain the verification elements of all nodes
SAODV	AODV	Dispatch public keys ofnodes	Digital signature , one-way hashchain	Whole packet	Intermediate nodes could reply routing request	High computational complexity due to asymmetric cryptograph
SLSP	ZRP	Dispatch public keys ofnodes	Digital signature, one-way hashchain	Whole packet	Prevent DoS attack by monitoring neighbor nodes	High computational complexity due to asymmetric cryptograph

REFERENCES

[1]. I.F. Akyildiz, X. Wang, W. Wang. Wireless Mesh Networks: a Survey . Computer Networks, Elsevier, Vol.47, No.4, 2005, pp445-487

[2]. Ping Yi, Yichuan Jiang , Yiping Zhong, Shiyong Zhang, security for mobile ad hoc networks, Acta Electronica Sinica, Vol.33, No. 5, 2005, pp893-899

[3]. Ping Yi, Yiping Zhong, Shiyong Zhang, Zhoulin Dai, Flooding Attack and Defence in Ad Hoc Networks, Journal of Systems Engineering and Electronics, Vol.17, No.2, 2006, pp410-416

[4]. Y-C Hu, A.Perrig, D.B.Johnso, Wormhole Detection in Wireless Ad Hoc Networks, Technical Report TR01- 384,Department of Computer Science, Rice University, December2001

[5]. Hongmei Deng,Wei Li and Dharma P.Agrawal, Routing Security in wireless Ad hoc Networks, IEEE Communications Magazine, pp.70-75, October 2002
[6]. Yih-Chun Hu, Adrian Perrig, and David Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003), September 19 2003, Westin Horton Plaza Hotel, San Diego, California, U.S.A.
[7]. 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 27-31,2002
[8]. Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Adhoc Networks, in Proceedings of the MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA
[9]. 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
[10]. https://jwcn-eurasipjournals.springeropen.com/articles/10.1155/2008/274790
[11]. https://www.cse.unsw.edu.au/~mahbub/PDF_Publications/mesh_2008.pdf
[12]. http://www.diva-portal.org/smash/get/diva2:306340/fulltext01.pdf
[13]. L. Eschenauer, V. Gligor and J. Baras \On trust establishment in mobile ad- hoc networks", in Proc. of 10th International Workshop on Security Protocols, Cambridge, UK, April 2002.
[14]. https://blackcloak.io/mesh-networks-benefits-and-impact-on-security/
[15]. https://arxiv.org/ftp/arxiv/papers/1302/1302.0939.pdf
[16]. Y. Desmedt, \Threshold cryptography", European Transactions on Telecommunication, vol. 5, no. 4, pp. 449-457, 1994.
[17]. P. De and S. K. Das, \Epidemic Models, Algorithms and Protocols in Wireless Sensor and Ad hoc Networks," Handbook on Wireless Sensor Networks, John Wiley, 2007.
[18]. P. De, Y. Liu and S. K. Das, \Modeling node compromise spread in sensor networks using Epidemic theory", in Proc. IEEE WOWMOM'06, pp. 237-243,Washington, DC, Jun. 2006.