iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI: http://doi.org/10.22214/ijraset.2020.4149

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Analysis of Routing and Secure Routing in Hybrid Wireless Mesh Networks

Ganesh Reddy Karri[1], Gunotham Solanki[2], Mohammed Yaseen Khan[3]
[1, 2, 3]*School of Computer Science and Engineering VIT-AP University, Amaravati, India,*

Abstract: Interoperability is one of the main characteristics of Hybrid Wireless Mesh Networks (HWMNs). In HWMNs, network devices have different resource constrains; identifying optimal paths over the heterogeneous environment is a challenging task. Reactive and proactive routing protocols of Ad-Hoc and sensor networks are ineffective in terms of scalability, thus researchers have come up with new routing protocols like cross-layer, and load-balancing protocols. However, these protocols fail to provide basic security to the network, a very few protocols have addressed the security in HWMNs, each of the secure protocol has its own limitations. In this paper, we analyze the issues in HWMNs routing protocols, and the security issues in proactive, reactive and hybrid protocols with respect to various network layer attacks. Based on our analysis, we have proposed the new research directions in terms of improving HWMNs routing functionality in the heterogeneous environment and new security dimensions for optimizing the network node resources and security mechanisms in HWMNs.
Keywords: Interoperability, wireless mesh, core layer attacks, detection, prevention.

I. INTRODUCTION

HWMN has becoming more popular because it has wide verity of applications like IoT, Ad-Hoc network, sensor network, and Vehicular networks. Network routers in HWMNs have different processing speed, queue size, energy levels, memory, and bandwidth constraints. Based on these constraints, network nodes are mainly classified into three types: Gateways, mesh routers (core routers), and clients. Gateways nodes support both wired and wireless connection other than internet connection. Mesh routers, most of the cases these are wireless routers with different capacities, form a backbone network. Mesh clients can be an ad-hoc node, IoT device, a sensor device, basically, these devices are different from conventional wireless devices[1][2]. Mesh clients support multi-hop communication and each client acts has router to forward the data in the client mesh network[3]-[6]. As per the current technology, two different client networks can't connect directly, but they can communicate through backbone mesh routers.

In HWMNs, network efficiency mainly depends on selecting the best route which has high throughput, low latency and less error rate to transmit the packets.

The existing classical routing protocols are mainly classified into three types: proactive, reactive and hybrid routing protocol. These routing protocols consider the hop count, bandwidth, and delay metrics to form a route between source and destination node. Once a route is established for data communication, this route is fixed for the entire communication [12]-[19]. On the other hand, computational intelligence routing protocols establish the paths based on congestion, trust, and load balancing metrics, in addition to this, these routing paths are updated based on the requirement.

The existing routing protocols are inefficient to support the complete interoperability of HWMNs. However, we use the existing protocols to run the applications over the HWMNs also topology of the network is highly dynamic due to mesh routers/clients are often join/leave the network at any time, these problems lead to various vulnerabilities at routing. Attackers identify the routing vulnerabilities to implement various types of control and data plane attacks. These attacks severely degrade the network performance if the existing routing protocols fail to address their security vulnerabilities. We mainly use intrusion prevention and detection approaches to address the vulnerabilities.

In intrusion prevention, we have studied existing proactive, reactive and hybrid secure routing protocols with respect to various network layer attacks. We studied specific trust-based routing protocols with respect to these attacks at backbone mesh and client mesh as the intrusion detection mechanisms. Based on our analysis, we have given the research directions which can mitigate the severity of the attacks. The rest of the paper as follows, section II demonstrates routing protocols issues, and Section III the explains intrusion prevention mechanisms and intrusion detection mechanisms, section IV elevates the research directions in terms of HWMNs security. Section V concludes this paper.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

II. ROUTING PROTOCOLS ISSUES IN HWMNS

The routing protocols in HWMNs are derived from both proactive and reactive protocols which are mainly used in Ad-Hoc and wireless sensor networks. The main objectives of the enhanced routing protocols are to address interoperability, load-balancing, SINR and channel interference in HWMNs. Due to heterogeneous network components and resource capacities; a single routing protocol may not suitable for all possible scenarios. Thus, many researchers have come up with new research dimensions on HWMNs routing protocols to address the HWMNs issues and optimize network performance.

The existing HWMNs routing protocols come under resource-aware routing protocols like bandwidth, queue size, processing delay, channel interference, etc.

Devaraj, D, et al. have proposed a wireless mesh routing protocol for Automatic Metering Infrastructure(AMI)[4]. The authors' have identified the issues in HWMP protocol and enhanced it by adding up new metrics like SINR, end to end delay, packet drops, and available bandwidth to form a route from the source node to the destination node. However, their work gives the best result for AMI which is a homogeneous network.

Aggregating workload and interference lead to degrading the network performance in HWMNs conventional routing protocol, yuan chain et al. have proposed a load-balancing routing protocol using a genetic algorithm[9]. Routing metrics like queue length, bandwidth, delay, node energy, and interference are considered in heterogeneous networks to transmit the packets in HWMNs. Gateway nodes and client network nodes use request and reply packets are used to collect the routing information in the network. This mechanism improves network performance by considering the cross-layer parameters to transmit the packets. However, this approach has poor convergence to find the best load-balancing path due to many routing metrics.

To improve the convergence rate, Yuan-chai et al. proposed a load-and interference balanced hybrid routing protocol in HWMNs[10]. In which, less resource constraint network components(routes) collect the information like available bandwidth, transmission delay, and queue length at backbone network, and mesh clients collect the node energy information. By using these resource metrics, mesh routers and clients calculate the weights of all available paths and choose the path which has the least value will be selected for data communication. This approach gives a poor performance as the mesh client network size increases.

Martin et al, have implemented the Interference-Disjoint Backup Paths to handle the dynamic traffic in wireless mesh networks[7]. Reactive Link-state routing protocol is used for inter-networking and proactive hop_count routing protocol is used for intra-networking. Both proactive and reactive routing protocols are used to form the disjoint paths in a network with a minimum number of control packets exchange.

The above routing protocols are derived from both reactive and proactive routing protocols to improve network performance. However, none of these routing protocols address the security issues in hybrid wireless mesh networks. Any compromised node advertises the fake information which can't be validated due to the absence of security in these protocols. Thus, the above mechanism is more vulnerable to various network attacks which are listed in table 1.

III. SECURE ROUTING IN HWMNS

In general, intrusion prevention systems and intrusion detection systems are used to detect and isolate the malicious nodes in the secure routing protocols.

A. Intrusion Prevention Systems (IPSs)

Intrusion prevention systems make use of symmetric and asymmetric keys to ensure the security characteristics: confidentiality, integrity and availability, apart from that these systems use traffic patterns to isolate the malicious nodes from the network.

1) *Network Layer Intrusion Prevention Systems: To protect against network layer attacks proactive, reactive, and hybrid secure routing protocols have been proposed. These secure routing protocols and their effects on various control plane attacks are explained below:*
2) *Secure Routing Protocols:* Secure Ad-hoc On demand Distance Vector (SAODV) protocol: SAODV is secure variant of AODV protocol which uses self-organized key management system to protect the routing metric from the internal and external attacks. SAODV depends on IPv6 protocol to select unique IDs of each and every node in the network [20]. In

SAODV, source node generates route request packet which contains mutable (hop_count) and non-mutable fields (control message). A mutable field is protected by the hash chain and non-mutable field is protected by the digital signature of each intermediate node in the route discovery path. Every time a node wants to send a Route REQuest (RREQ) or a Route REPly (RREP) packet, it selects the maximum hop_count seed in equation 1.

$$Top\_Hash = h^{Max\_Hop\_Count}(seed) \quad (1)$$

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

Every time a node receives a RREQ or a RREP packet, it will verify the hop_count of the message. Before rebroadcasting a RREQ or forwarding a RREP packet, it creates a hash of hashes for the signature extension in equation 2.

$$Top\_Hash = h^{Max\_Hop\_Count - Hop\_Count(seed)} \quad (2)$$

When a node has a route to the destination, it generates a RREP packet with double signatures (RREP packet is signed by intermediate node and destination node). The double signature verification of each request/ reply packet needs more CPU time. Moreover, self-organized key management mechanism is more vulnerable to colluding attacks such as blackhole, grayhole, wormhole attacks etc., because no centralized authority to control the internal colluding attackers. For example, colluding attackers are able to create blackhole attack by forwarding a RREQ or a RREP packet without increase the hop_count.

Secure Routing Protocol (SRP): SRP is a secure variant of DSR protocol uses secret sharing mechanism to prevent external DoS attacks. Prerequisite shared secret key K_{sd} is required between the source and destination nodes before route discovery starts [26]. This process has less communication and computational overhead because intermediate authentication is required only when route reply is generated for the destination node. In the process of SRP, route request packet contains < Soure IP, Destination IP, ID, SN and gt>, and it is signed by shared secret key K_{sd}. Source node disseminates the RREQ packet which will be forwarded by intermediate nodes until it reaches to the destination node. Destination verifies the route request with K_{sd} and verifies the sequence number (SN) to confirm whether this packet is

new or old. Once the verification is done, destination node creates route replay (RREP) which contains <Source IP, Destination IP, ID, SN, intermediate nodes &gt> and it is signed by K_{sd} then unicast RREP in reverse route to the source node. Source node verifies RREP packet with a shared secret key to detect alteration in RREP packet by the malicious node. SRP is more vulnerable than SAODV, because a single attacker can forward the RREP packet without incrementing/ decrementing the hop_cont to create blackhole attack. In addition, all attacks which are possible in SAODV also possible in SRP.

Secure Link State Routing Protocol (SLSP): SLSP protects link state update (LSU) and topological maintenance information about nodes which are in the same zone [27]. It prevents from authentication attacks such as IP forging attack, masquerading attack and detects the flooding attacks such as hello packet flooding by using threshold parameter. A self-organized public key cryptosystem is used here to authenticate the neighboring nodes i.e., to do this every node has to select its own public key and disseminate periodically to its neighbors. Each node public key is certified by its neighbors, therefore, each of the link state updates (LSU) are signed by this certified public keys. It calculates a one-way hash chain to make sure LSU are propagated within the zone

of origin. To prevent the DoS attacks, each node broadcasts its (IP, MAC) in the form of signed hello messages. SLSP is vulnerable to a group of internal attackers. For example, a group of internal attackers can isolate the legitimate node from the network by sending false LSU to other group members. Other internal control plane attacks are also easily possible when group of attackers work together.

Secure Efficient Ad-hoc Distance vector (SEAD) routing protocol: SEAD protocol is mainly focused on four functionalities such as i) metric and sequence number authentication, ii) neighbor authentication iii) preventing same-distance fraud and iv) bounding verification overhead [25]. To provide confidentiality, integrity and authenticity, SEAD protocol uses one-way hash chains, merkle hash trees and shared secret key mechanisms. Authenticator (source node) uses one-way hash function to protect against multiple uncoordinated attackers. To prevent same-distance fraud attack, authenticator uses merkle hash tree chains. Any two neighboring nodes' authentication is done by shared secret key. In SEAD protocol, attacker can attempt or reduce the amount of routing information available to other nodes by not advertising certain routers or by destroying routing paths. In addition, this protocol is vulnerable to all internal colluding attackers.

Secure Hybrid Wireless Mesh Protocol (SHWMP): SHWMP is secure variant of HWMP which uses hop-by-hop authentication on the mutable fields using a Merkle tree [21]. This protocol assumes the availability of keys via IEEE 802.11s security framework and utilizes IEEE 802.1X for initial authentication. SHWMP protects control plane packets such as path request (PREQ), path reply (PREP) and route announcement (RANN). These packets have routing information elements in which mutable and non-mutable elements exist. All the mutable elements of PREQ, PREP, and RANN are protected by authenticated one way-hash using the concept of mekrle tree. Non-mutable elements of PREQ, PREP, and RANN protected by using symmetric key cryptosystem. In SHWMP colluding attackers affect all mutable fields, and all attacks possible in SAODV are possible in SHWMP because these two are working on same principle called mutable fields and non-mutable fields security.

AntSec: It is a proactive, probabilistic, multipath, st- igmatic-based, distributed and non-broadcast based secure routing algorithm in WMN security framework. Antsec discovery forward ant (DFANT) contains registration certificate and public key to authenticate source node [32]. Each intermediate node requests the registration certificate and public key of the destination on forwarding route. Maintenance forward ant (MFANT) message is used for update the current routes. Backward ant (BANT) message is generated by destination node which contains its registration certificate and the public key of this node. BANT message guarantee the integrity by

being signed by destination node which will verify by the intermediate nodes on backward path. Moreover, WMN security framework uses intrusion detection (watchant) and reputation (antrep) solutions which are explained in next section. In AntSec, hop_count field is vulnerable to internal attackers when the nodes are failed to receive routing updates in a timely manner.

Authenticated Routing for Ad-hoc Networks (ARAN): Authenticated Routing for Ad-hoc Networks (ARAN) protocol objective is to provide end-to-end authentication [23]. It is a secure variant of AODV and DSR protocols. The prerequisite condition of ARAN is to have trusted centralized certification server to distribute certificates. These certificates are revoked when they expire. In the process of renewing these certificates, ARAN protocol creates more network overhead. In ARAN, authenticated route discovery process is initiated by source node S for a particular node D (destination). Here, source broadcasts Route Discovery Packet (RDP) which contains the following fields: IP address of the destination (IP_D), S certificate ($Cert_S$), nonce (N_S), and the current time (t) signed with S private key K_S. The receiving node A of RDP uses S public key, which it extracts from S certificate, to validate the signature and verify that S certificate has not expired and on A's private key K_A, appends its certificate CertA. This process continues until RREQ message reaches to the destination. Once it reaches to destination node D, it verifies the intermediate node certificates and signatures then it forms a reverse route called REply Packet (REP). The destination node D signs on the REP packet and follows similar process of RDP to forward REP to source node S along with the reverse path. ARAN is more vulnerable to colluding attackers as compared to any other security routing protocols because every intermediate node first authenticates by it neighboring nodes. Here, all neighboring nodes can act as colluding attackers to isolate the target nodes from the network.

A secure on-demand routing protocol for Ad-hoc networks (Ariadne):} Ariadne is secure variant of DSR and protects using TESLA [24]. TESLA is a broadcast authentication protocol for authenticating routing messages. Every message has message authentication code (MAC) to provide a secure authentication in point-to-point communication. To prevent other nodes from forging MAC, each node needs time synchronization and delayed key discloser.

The prerequisite conditions of Ariadne initializes pairwise secret keys, shared keys between all source and destination pairs and their clocks must be synchronized. In Ariadne, source node computes delayed key also called TESLA key to encrypt MACs of sending messages. Destination node buffers all messages until source node release the delayed key and then verifies it by using the key. Time synchronization is required to protect the MAC and delayed key. It can protect the wireless network from internal rushing attack because it provides time synchronization for packet verification at he destination node irrespective of source information. However, the major problem of Ariadne is not being integrated with decentralized systems.

Table 1. shows the analysis of secure routing protocols against control plane attacks. Whereas blackhole, wormhole,grayhole, routing loop, rushing and location discloser attacks are the internal attacks which are discussed in our paper "Taxonomy of Network Layer Attacks in Wireless Mesh Network"[17]. All these attacks have enough privileges to participate in the routing functionalities. To participate in active route, single attacker can create blackhole and grayhole attacks by not incrementing the hop_count in SRP, SEAD, SHWMP, SAODV, and SLSP protocols because hash of the mutable field only look at the modification of hop_count. AntSec, ARAN, and Ariadne is less vulnerable to blackhole and grayhole attacks because destination node verifies the certification of all intermediate nodes in the active route but these security protocols are not adequate to block blackhole and grayhole attacks. Wormhole attack by

colluding attackers can gain the active route by broadcasting very low latency routes in the network. However, existing secure routing protocols do not consider the packet delay between two nodes.

Location discloser attack cannot be prevented because any internal node intentionally can broadcast the topology information in the network. Rushing attack is prevented by ARAN, Ariadne, and SEAD because it follows the time synchronization between nodes. However, ARAN, Ariadne and SEAD do not have countermeasure for blackhole, wormhole, grayhole, sybil and location discloser attacks. Routing loop attack, replay, flooding, route cache and sybil attack are the external attacks of the control plane. To prevent external attacks, all the security routing protocol provides robust security services by using long keys and strong encryption algorithms.

Due to this reason, replay attack is not possible and route looping attack is avoided because of protected sequence number and TTL by all secure routing protocols. Sybil attacker steals the legitimate user identities or uses the stale identities of the legitimate user to participate in different routes of inter-network.

This attack is also not addressed by any secure routing protocols. Route cache poisoning and flooding external attacks can be avoided because authorized nodes participate in route discovery and route maintenance phase. Existing IPSs are inadequate to protect against internal attacks which leads to data plane attacks in the network layer, along with IPSs we need Intrusion Detection Systems(IDSs).

Attacks/Security protocols	SAODV	SHWMP	AntSec	ARAN	Ariadne	SEAD	SRP	SLSP
Blackhole	NO	NO	NO	NO	NO	NO	NO	NO
Wormhole	NO	NO	NO	NO	NO	NO	NO	NO
Grayhole	NO	NO	NO	NO	NO	NO	NO	NO
Location Discloser	NO	NO	NO	NO	NO	NO	NO	NO
Sybil	NO	NO	NO	NO	NO	NO	NO	NO
Rushing	NO	NO	NO	YES	YES	YES	NO	NO
Routing loop	YES	YES	YES	YES	YES	YES	YES	YES
Replay	YES	YES	YES	YES	YES	YES	YES	YES
Flooding	YES	YES	YES	YES	YES	YES	YES	YES
Routing cache poisoning	YES	YES	YES	YES	YES	YES	YES	YES

B. Intrusion Detection Systems(IDSs)

In section III-A, we have explained the secure routing protocols which are adopted from ad-hoc, sensor and wireless mesh networks. In this subsection, we study the HWMN IDSs for secure routing.

In recent years, few of the IDSs security protocols have been proposed to address the issues in hybrid wireless networks.

Badis Hammi et al. proposed a multi-path routing protocol in IoT and HANET[1]. Initially, trust nodes calculate and maintain the trust of their neighboring nodes, the trust value of a node will be considered to find the complete path of trust. All possible multi-paths trust will be calculated by these node trust values. Out of all the available paths trust values, a path that has the highest trust value is selected for data communication. In this approach, trust nodes process insufficient data to detect the malicious nodes thus, there is inaccurate trust values of different paths that exist.

Navmani T M et al. proposed a trust-based secure routing to prevent network layer attacks. Node authentication is implemented to prevent external attackers[2]. Then, all authenticated node behavior is monitored in different layers such as MAC, network and physical layer by the trust nodes. Trust nodes assign reputation values to all authentication nodes. If any node reputation values are below the threshold value, then the node immediately isolates this node from the complete network. This approach takes more time identify the trusted paths and resource consumption of a node is very high compare with other IDSs.

Ganeshan A et al. have proposed privacy-preserving secure routing protocol in wireless mesh networks. The ant-based trust model is used to establish the secure paths between the source and destination nodes, in which every node in a network calculates the trust value of its neighboring nodes by considering their cooperativeness and packet loss rate[8]. A node that has the highest trust value will be selected as a forward (next) node. Mobile clients use the tri-lateral pseudo-random numbers to join the network along with the conventional authentication mechanism. However, this approach does not consider the cross-layer metrics to validate the malicious node behavior, thus, false positives and false negatives more when compared with other security models.

Existing IDSs for secure routing are inadequate in terms of reducing the false positive, false negatives, convergence and effective resource utilization.

IV. RESEARCH DIRECTIONS

In this section, we have listed out research direction on routing and secure routing protocols.

A. HWMNs Routing protocols

Based on the resource constraints of mesh routers and clients, HWMNs routing protocols can be either proactive, reactive, or hybrid protocol. Primarily, HWMN nodes are classified into different regions based on its resource constraints, we have recommended the reactive, proactive and hybrid protocols in the following scenarios.

1) Reactive routing protocols are more efficient for a region that has highly dynamic topology with more resource constraints like bandwidth, queue size, and processing delay. In general, client mesh network has dynamic topology and very high resource constraints, so reactive protocols can be used for client mesh networks.

2) Proactive routing protocols are more efficient for a region that has static in topology with negligible resource constraints like bandwidth, queue size, and processing delay. In general, gateway nodes have equipped with more resources and the static nodes, so proactive protocols can be used for gateway nodes communication.

3) Hybrid routing protocols are more efficient for a region that has moderately change in the topology and fewer resource constraints like bandwidth, queue size, and processing delay. In addition to this, hybrid routing protocols consider cross-layer metrics, also train these metrics by using machine learning algorithms to select the best paths for communications. In general, backbone mesh routers have less resource constrains and handles the heavy and highly fluctuating network traffic; here, reactive and proactive protocols are inefficient, and the only solution is to apply hybrid routing protocols.

B. Secure Routing Protocols

Based on our analysis in section III on secure routing protocols, we have recommended the following research directions to secure the HWMNs network.

1) New secure routing protocols need to be developed to prevent/mitigate the internal colluding attacks such as blackhole, gryhole,sybil, wormhole, jellyfish and byzantine attacks.

2) The secure routing protocols need to be adaptive in backbone mesh as well as client mesh. In addition to this, these routing protocols need to have minimum communication and computational overhead.

3) In IPSs, cryptographic functionalities such as confidentiality, integrity, and availability have been selected based on the resource constraints of the backbone mesh and client mesh networks.

4) Cross-layer IDS can reduce the false positives and false negatives, these values are further reduced by implementing the reputation mechanism. However, this type of IDSs won't give the effective result on the client mesh, so a single layer IDS without a reputation mechanism will be the best solution on the client mesh network.

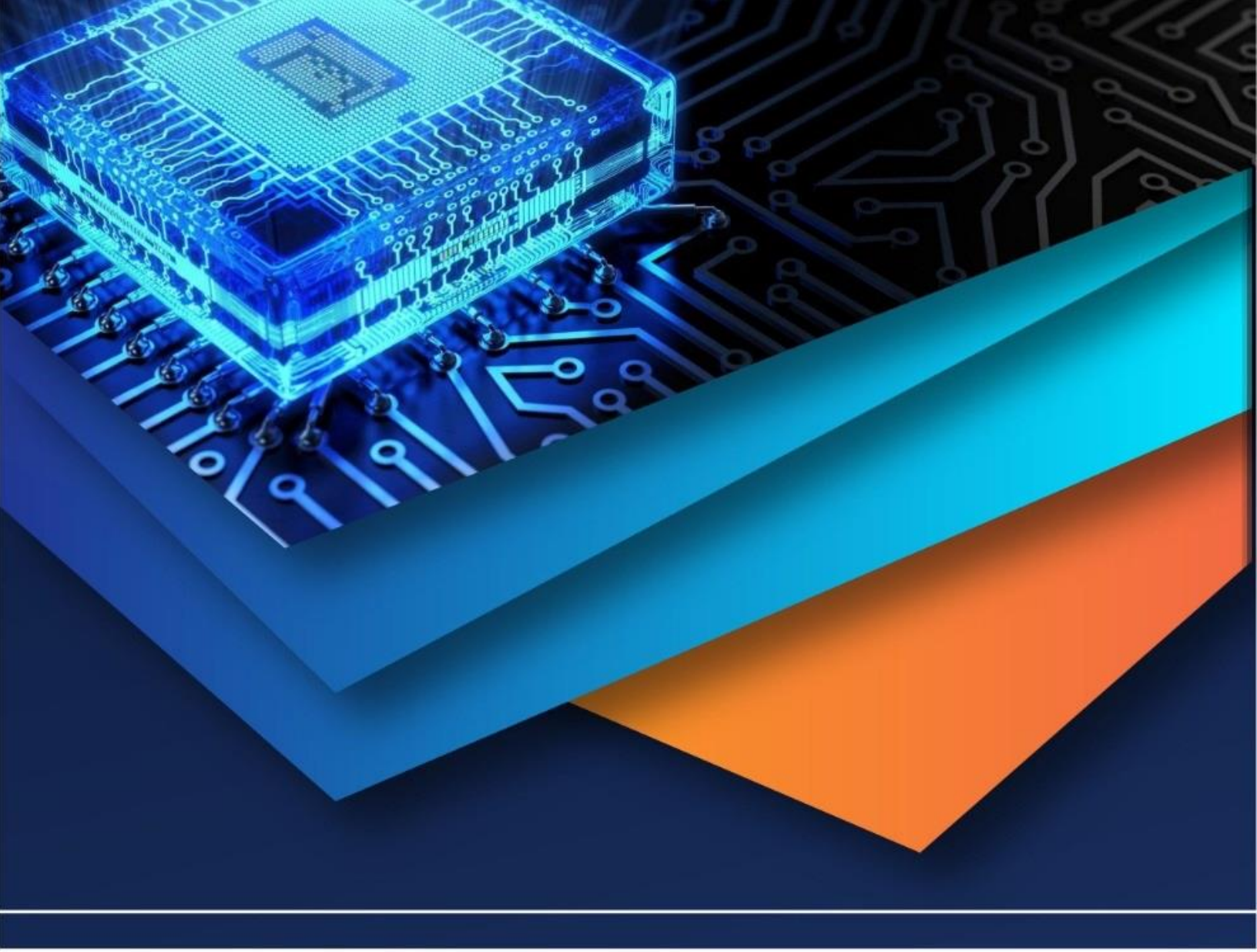
V. CONCLUSION

In this paper, we have analyzed various HWMNs and Ad-Hoc secure routing protocols and identified the limitations of different secure routing protocols performance with respect to the network layer attacks. Based on our analysis, we identified that there is a very much need of robust intrusion prevention systems (IPSs) and intrusion detection systems (IDSs) to protect HWMNs from various attack, and very few solutions have been proposed which includes both of the intrusion prevention and intrusion detection solutions. However, all these solutions are inadequate to protect interoperability feature of HWMNs in the hostile environment. We have proposed new research directions for upcoming solutions and strengthening the existing IPSs and IDSs of HWMNs.

REFERENCES

[1] Hammi, Badis, et al. "A Secure Multipath Reactive Protocol for Routing in IoT and HANETs." Ad Hoc Networks (2020): 102118.
[2] TM, Navmani. "Trust based Secure Reliable Route Discovery in Wireless Mesh Networks." KSII Transactions on Internet & Information Systems 13.7 (2019).
[3] Reddy, K. Ganesh, M. S. Sudheer, P. Kiran Sree, and V. Purushothama Raju. "Simulation analysis on network layer attacks in wireless mesh net-works." International Journal of Engineering and Technology 7, no. 3.29 (2018): 301-303.
[4] Devaraj, D., and R. Narmatha Banu. "Genetic algorithm-based optimisation of load-balanced routing for AMI with wireless mesh networks." Applied Soft Computing 74 (2019): 122-132.
[5] Chai, Yuan, and Xiao-Jun Zeng. "Load-and Interference-Balance Hybrid Routing Protocol for Hybrid Wireless Mesh Network." 2019 Wireless Days (WD). IEEE, 2019.
[6] Chai, Yuan, and Xiao-Jun Zeng. "Regional condition-aware hybrid routing protocol for hybrid wireless mesh network." Computer Networks 148 (2019): 120-128.
[7] Backhaus, Martin, et al. "Robust and Scalable Routing in Wireless Mesh Networks Using Interference-Disjoint Backup Paths." 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC). IEEE, 2019.
[8] Akilarasu, Ganesan, and S. Mercy Shalinie. "Privacy preserving protocol for secure routing in wireless mesh networks." International Journal of Mobile Network Design and Innovation 8.1 (2018): 54-59.
[9] Chai, Yuan, et al. "An efficient cooperative hybrid routing protocol for hybrid wireless mesh networks." Wireless Networks 23.5 (2017): 1387-1399.
[10] Chai, Yuan, Wenxiao Shi, and Tianhe Shi. "Load-aware cooperative hybrid routing protocol in hybrid wireless mesh networks." AEU-International Journal of Electronics and Communications 74 (2017): 135-144.
[11] Lin, Hui, et al. "A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks." Computers \& Electrical Engineering 64 (2017): 407-419.
[12] Nanda, Ashish, et al. "A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks." Future Generation Computer Systems (2018).
[13] K. Ganesh Reddy, Syni M, "Intrusion detection system for Rushing attack in MANETs" International Journal of Merging Technology and Advanced Re-search in Computing (IJMTARC), vol:4 and issue-16, page no:1-7(2016).

[14] Kumar, S. Ashok, E. Suresh Babu, C. Nagaraju, and A. Gopi. "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET." International Journal of Electrical \& Com-puter Engineering (2088-8708) 5, no. 5 (2015).
[15] K. Ganesh Reddy, P. Santhi Thilagam(2014), "Reputation based Cross-layer Intrusion 12. Detection System for Wormhole Related Attacks in Wireless Mesh Networks" Security and Communication Net-works-Journal-Wiley, Volume no: 7, pages 2442–2462, doi: 10.1002/ sec. 955.
[16] Reddy, K. Ganesh, and P. Santhi Thilagam. "Hierarchical Wireless Mesh Networks Scalable Secure Framework." International Journal of Information and Network Security (IJINS) Volume 2 (2013): 2.
[17] K. Ganesh Reddy, P. Santhi Thilagam (2012). "Taxonomy of Network Layer Attacks in Wireless Mesh Network." Advances in Computer Science, Engineering and Applications. Springer, Advances in intelligent systems and computing Volume no:167, Page no:927-935.
[18] I.F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Computer networks, Elsevier 47 (4) (2005) 445-487.
[19] J. Xie, X. Wang, A survey of mobility management in hybrid wireless mesh networks, Network, IEEE 22 (6) (2008) 34-40.
[20] Lu, Songbai, et al. "SAODV: a MANET routing protocol that can withstand black hole attack." 2009 international conference on computational intelligence and security. Vol. 2. IEEE, 2009.
[21] Islam, Md Shariful, Md Abdul Hamid, and Choong Seon Hong. "SHWMP: a secure hybrid wireless mesh protocol for IEEE 802.11 s wireless mesh networks." Transactions on Computational Science VI. Springer, Berlin, Heidelberg, 2009. 95-114.
[22] Mogre, Parag S., et al. "AntSec, WatchAnt, and AntRep: Innovative Security Mechanisms for Wireless Mesh Networks." 32nd IEEE Conference on Local Computer Networks (LCN 2007). IEEE, 2007.
[23] Mahmoud, Abdalla, Ahmed Sameh, and Sherif El-Kassas. "Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)." IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.. IEEE, 2005.
[24] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless networks 11.1-2 (2005): 21-38.
[25] Hu, Yih-Chun, David B. Johnson, and Adrian Perrig. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks." Ad hoc networks 1.1 (2003): 175-192.
[26] Marshall, John. "An analysis of SRP for mobile ad hoc networks." Proceedings of the 2002 International Multiconference in Computer Science. 2002.
[27] Ho, Pin-Han, and H. T. Mouftah. "SLSP: A new path protection scheme for the optical Internet." OFC 2001. Optical Fiber Communication Conference and Exhibit. Technical Digest Post conference Edition (IEEE Cat. 01CH37171). Vol. 2. IEEE, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY