Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

Cross-Layer Intrusion Detection in Mobile Ad Hoc Networks – A Survey

Naresh Kumar Trivedi[1], Ajay Kumar[2], Abhineet Anand[3], Shikha Maheshwari[4]
1, 2, 3 & 4 - Chitkara University Institute of Engineering Technology, Chitkara University, Punjab.
1-nareshk.trivedi@chitkara.edu.in, 2-akumar@chitkara.edu.in, 3-abhineet.anand@chitkara.edu.in,4-shikha.maheshwari@chitkara.edu.in

Abstract: In MANETS (Mobile Ad Hoc Networks), prevention methods are not sufficient to make them secure. Shared medium in wireless networks makes it much more vulnerable to attacks. Intrusion detection adds to another layer of defense. Detecting intrusion by analyzing the information gathered at other layers of protocol stack as well increases the probability of detection. In this paper we present the survey of cross-layer intrusion detection schemes for MANETS. Main features for each of these schemes are described briefly, followed by a few observations. Directions for future research are presented at the end.

Introduction:
A MANET is a collection of mobile wireless nodes that can communicate with one another without the us e of network infrastructure or any centralized administration. Besides the wide range of attacks similar to those performed in wired networks, mobility, limited bandwidth and limited battery life offer opportunitie s to launch new attacks.
Certain DoS attacks occur at more than one layer. Some of these attacks may not be detected with certainty looking to the intrusion information gathered at a single layer of a protocol stack[1].

Layering in protocol stack, as is done in OSI, has two disadvantages, first it is inflexible, and second it may not be offering optimal solution. Layering is inflexible because any application has to depend on the functionality of layers underneath. Layers do not have complete information of network and hence the functions performed by layers in a wireless network may not be offering optimal solution. Layers in a wireless network must synchronize and adjust with the change in the different state of the wireless network.

The cross-
layer architecture of the protocols requires layers to swap state information to accommodate the changes i n wireless network status. Sharing network information among layers allows each layer
to get a global picture of the network's constraints and characteristics.
The adaptation of changing state of network leads to better co-ordinations amongst layers and activate them to take decisions that would be improved the performance of the network[2][3].

2. Classification of Intrusion Detection Schemes: A number of Intrusion Detection schemes have been proposed with varying objectives of Intrusion detection. Though these schemes can be classified on a number of parameters like approach of intrusion detection (anomaly detection or rule-based detection), structure (centralized or decentralized), audit source (host-based or network based), and so on, here we arrange some of the schemes proposed in the different research papers in the order of rule-based intrusion detection followed by Anomaly based intrusion detection[1], [4].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

3. Rule-based Intrusion Detection Schemes:

3.1 Scheme proposed by Geethapriya Thamilarasu, Arun Balasubramanium, Sumita Mishra, Ramalingam Sridhar[5];

In scheme proposed by Geethapriya & el., DoS attacks due to packet dropping, packet misdirection at network layer and nodes causing collision at link layer have been dealt with. By using cross-layer approach, it is possible to detect the misbehaving node with low false alarms.

Each node in the network gathers raw information for intrusion detection at routing (network), link and physical layers. Intrusion detection takes place at two layers of OSI protocol, namely routing layer and link layer. Cross-layer detection takes place in two forms, first by analyzing detection information from a layer along with detection information from other layers, and second by analyzing raw information received from other layers along with raw information of this layer. First form of detection is christened as CIDS-I and second form as CIDS-II by the authors.

Table 3.1 Summary of Scheme proposed by Geethapriya et al.[5]

Layer	Information Provided by a layer to IDS	Information used by Layer	Action taken by IDS
Physical	Battery (Energy) Level	Routing Layer of neighboring nodes.	If energy level is low, broadcast a message that node cannot participate in normal functioning due to low energy level. Such a node may be able to receive messages, but will not be able to forward or transmit messages.
Link Layer	1.Collision while transmitting a message 2.Available buffer space with a node	Link Layer Routing Layer	1.1 Transmitting node selects a node within its transmission range as "monitor". 1.2 "Monitor" node submits a list (known as hit list) of possible defaulters for causing collision to the transmitting node. 1.3 Transmitting node computes a list of nodes, which occur frequently in from above hit lists. 2. A Node should participate in forwarding of RREQ packets only if enough buffer space is available.
Routing (Network)	By using "watchdog" mechanism, a node detects dropping or misdirection of packets by neighbor nodes. 1. If suspected of misbehavior due to packet dropping.		1. Checks if the low energy level signal was received from the misbehaving neighbor. 1.1 If yes, node is not termed as misbehaving as packet drop is due to low energy level.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

			1.2 If no, check if enough buffer space is available at next node. Monitor* node generates a dummy RREQ to the same destination. 1.2.1 If the suspected node responds with RREP, then the suspected node has enough buffer space at its link level, and hence packet drop is intentional, and monitor node increments the counter of misbehavior for suspected node. 1.2.2 If the suspected node does not respond with RREP, then it may not be having enough buffer space at link-layer, hence it remains in suspicious state only.
	2. If suspected of misbehavior due to misdirection of packet.		2. If node to which packet has been forwarded is not same as suggested by DSR protocol, then monitor node increments the counter of misbehavior for suspected node. (For other protocols like AODV, DSDV, OLSR, TBRPF etc. modifications are required in the in the scheme as next hop is not known to node keeping a watch).
	3. Normal behavior		3. If node has forwarded the packet to the desired node, then (watchdog) monitor node decrements counter of misbehavior for the node, subject to lowest value as zero. This decrease in counter value may bring an erring node into the range of acceptable misbehavior level for nodes.

Information provided by link layer to Intrusion detection module of that node:

1. Any node while transmitting a message to another node cannot detect collisions, if any, with its ongoing transmission. In this scheme, every sender node selects another node within its transmission range to monitor collision(s) and pass on a list of suspected nodes, which could have caused this collision to the packets sent by this sender node. This monitoring takes place at link layer and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

intrusion detection module at every node keeps on collecting lists of nodes. A node, which repeats in most of these lists, is a suspicious node.

2. In addition to this, link layer provides information regarding available buffer space at that node. A node is supposed to respond to RREQs only if sufficient buffer space is there[6].

Information provided by routing layer to Intrusion detection module of that node:
By using "watchdog" [9] mechanism, a node monitors the behavior of other nodes within its transmission range that are involved in the forwarding of a message. Thus nodes with suspicious activities of packet dropping, and/or packet misdirection are observed at routing layer. In this scheme, precaution is taken that packet drop due to genuine reasons like lack of buffer space at link layer or low battery power do not consider it as a misbehavior. However, if none of these two conditions is satisfied, and the node is consistently dropping packets, then it is termed as a misbehavior. When a node has battery level lower than a threshold, that is energy level is less than required to forward a package, it transmits a control signal informing its neighbors indicating a low battery. Thus if low battery signal has been received from a neighboring node and that node is dropping packets, then it is not termed as a misbehavior. Further, monitoring node will generate a RREQ for the same destination. Any node is not supposed to forward RREQ if it does not have sufficient buffer space at link layer. If the suspicious node does respond to RREQ generated by monitor node, then it is certain that enough buffer space was available at the suspicious node and hence packet dropping was intentional. By using DSR algorithm, where the source node decides the next hop, it is possible to determine the packet misdirection by another node by "watchdog" mechanism[7].

Authors prove that (i) probability of having a good node as a monitoring node when good nodes outnumber the misbehaving nodes is more than zero, and (ii) by selecting a different monitor node each time a collision occurs, a misbehaving monitor node cannot detract the IDS.

This scheme has to be extended to (i) adapt other routing protocols like AODV, DSDV, OLSR, TBRPF, and so on, (ii) express packet drop due to poor channel conditions leading to scattering, path loss and reflection, in a measurable mathematical form, (iii) generate suitable intrusion response, (iv) allow measurement of congestion on the basis of product of time for which a packet remains in buffer and the number of packets in buffer, rather than the number of free buffer space available.

3.2 Scheme proposed by Jarmo V.E. Molsa

In this paper two cross-layers designs have been proposed to mitigate the range attack, which is a new type of DoS attack.

In these types of attacks, no node may be compromised. Attacker by getting very close (physically) to the attacked node changes the properties of its antenna in any one way of the two types of range attacks: (a) the attenuating range attack, (b) the amplifying range attack. These type of attacks persist for a sort period of time but may be repeated at regular/irregular intervals[8].

In attenuating range attack the transmission range for the attacking node is decreased for a short period of time repeatedly at regular or irregular intervals. This causes regular break-ups in the multi-hop connections passing through the attacked node.

The routing layer and the MAC layer should
have the following overlapping characteristics with respect to range attack:

- These two layer can have different bidirectional requirements.
- Routing and MAC layer can carry out bi-directionality tests.
- Identification of transmitted messages could be applied by both layers.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

• Routing and MAC layers can detect hyperlinks

All these features should be coordinated, and a cross-layer design is one possibility for this.

The proposed cross-layer design ensures that routing layer does not accept routes with unidirectional links as MAC Layer operating with IEEE 802.11 does not accept such links. Thus information from MAC layer should be passed on to routing layer.

In Amplifying range attack the transmission range of a node is increased, for example, by converting an omni-directional antenna into a directional antenna. Since communication link has become unidirectional and it continues to accept packets for delivering on both directions, so it acts like a "sink hole" for one direction.

Both the types of range attacks (attenuating and amplifying) require that due to change of link properties there are large variations in the routing table. The selected routes should not have uni-directional links; otherwise the effect of range type of attacks would be prominent.

Some times because of node mobility, a critical link breaks and the messages queued at TCP layer cannot be forwarded. If a request sends time-sensitive information that should be transmitted within a specified maximum delay, then a request will wait for full acknowledgment of the previous transmission before sending out a next messa ge.

So the cross-layer design for the amplifying type of range attack involves sharing of TCP acknowledgement between application and TCP layers. Application layer is prevented from sending new time sensitive until previous message is acknowledge by TCP layer.
Alternatively, we can use SCTP (Stream Control Transmission Protocol). SCTP blocks delivery of packets with higher sequence numbers, even if these packets have been received correctly, when a lower sequence number packet has been lost.

Table 3.2: Range Attacks, Summary of Scheme proposed by Jarmo V.E. Molsa [8]

Layer	Information Provided by a layer to IDS	Information used by Layer	Action taken by IDS
Routing (Network)	Uni-directional links are not accepted if MAC layer requires bi-directional links (e.g., IEEE 802.11 at MAC layer)	MAC Layer	This is necessary for mitigating and preventing attenuating and amplifying types of range attacks. Cooperation between routing & MAC layers makes it possible to detect inconsistencies between the desired properties of these two layers in the form of implementing acknowledgements and detection of link status such that the information is acceptable to protocols implemented at these layers.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

	Share TCP acknowledgement status with an application.	Application Layer	When transmission of messages is relatively infrequently, it is a sign of an unavailable end-to-end path (possibly due to range attack). Keep an application from sending new time-delicate information while past TCP-level messages are not yet perceived. In any case another message would just stay in a send cradle sitting tight for an utilitarian end-to end way, and the message would gradually pointlessly lose its idealness and waste system assets during this period.

3.3 Scheme proposed by Svetlana Radosavac, John S. Baras, Nassir Benamma

In this paper the focus is on DoS attacks which aim to partition the network. Attack detection is based on modeling of MAC protocol (IEEE 802.11) using Extended Finite State Machines (EFSM) and the validating communication patterns in the network according to the modeled MAC behavior. In this paper only IEEE 802.11 protocol of MAC layer has been modeled using EFSM. It helps in detecting misuse of backoff counter, contention widow, start of transmission before completion of DIFS time, that is, misbehavior at MAC layer, selfish or otherwise is detected. Detection of such types of misbehavior at MAC layer prevents problems at routing layer. Moreover, any misbehavior at MAC layer is reported to IDS of the node[9].

Further, MAC layer passes information regarding congestion and interference to routing-layer. Routing-layer in turn will select out of possible routes from a source to a destination, which are bi-directional only as is the requirement of IEEE 802.11 protocol at MAC layer. Since both these layers communicate with IDS as well, IDS will make sure that selected route does not contain malicious nodes.

The goal of this scheme is to maximize the probability of detection while keeping intrusion detection time and number of false alarms as minimum.

Table 3.3: Summary of EFSM scheme by Svetlana Radosavac et al. [9]

Layer	Information Provided by a layer to IDS	Information used by Layer	Action taken by IDS
MAC Layer	Congestion and interference If communication pattern differs from the modeled EFSM, that is, misuse of either of backoff timing, NAV, CW etc. for selfish or malicious behavior.	Routing Layer	Routing layer will propose routes that do not have congested links and IDS will avoid malicious nodes detected so far in new proposed route(s). Any suspected behavior will make IDS to get global information before declaring a node as malicious.
Routing	A number of possible routes to a destination	MAC Layer will reply back with routes having less	IDS will avoid malicious nodes detected so far in the new routes.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

		congestion and interference.	

It may be pointed out that a robust algorithm for detection of colluding nodes needs to be worked out. Moreover, measurement of congestion and interference needs to be specified in more clear terms. EFSM modeling of other MAC protocols should also be worked out.

3.4 Scheme proposed by Yongjin Kim, Ahmed Helmy

In this scheme traceback of DoS/DDoS attacker victimizing a particular node by sending large number of packets is done by cooperation at MAC and Network layers. It is observed that DoS/DDoS attacks victimizing a node with large number of packets have: (1) High Traffic volume during attack period. (2) Attackers hide their location by using dummy addresses. (3) Duration of such attacks may be short or long periods. By looking at first two characteristics of the attack pattern, this scheme proposes that any packet moving around the network should have two parameters, (1) destination address, which is part of routing layer, and previous hop MAC address, which forms a part of MAC layer information[10].

"Assault signature" is characterized as time arrangement information of approaching Macintosh Layer outline include in k time allotments. Irregularity is distinguished by utilizing Partial Deviation from the Mean (FDM) or other measurable strategies. For the purpose of obtaining accurate attack signature, there is need to reduce/remove the background (normal) traffic. By network layer information, that is, the destination address, some part of the noise in attack signature can be reduced (this noise is also known as forward noise). By MAC layer information, that is, previous hop MAC address, some other part of noise in attack signature can be removed (this noise is called backward noise). Each node maintains its own attack signature table, which is the abnormal increase of packets to a particular destination from a particular route. At whatever point assault is identified by interruption recognition arrangement of a casualty, the victim describes the assault signature. Victim sends a question with its assault mark to its contacts (a lot of hubs that transfer inquiry to its region hub) to discover moderate hubs that watch comparative variation from the norm in assault signature. Figure above shows the follow back system for a given assault signature.

Each contact accumulates anomaly data from its region hub and figures the assault vitality. By finding the biggest assault vitality on a contact hub, it is conceivable to discover the locale the assault traffic navigated. Spatial area around assailant shows high assault signature vitality esteem. The vitality is influenced by level of hubs watching mark vitality, middle good ways from the objective, and normal individual mark vitality in a spatial locale. Thus the search process continues towards attack origin. When there are no more contact report or no different hubs outside the region, the last contact reports the total assault course to the person in question. It is conceivable to utilize multi-directional quest for DDoS aggressor follow back[11].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

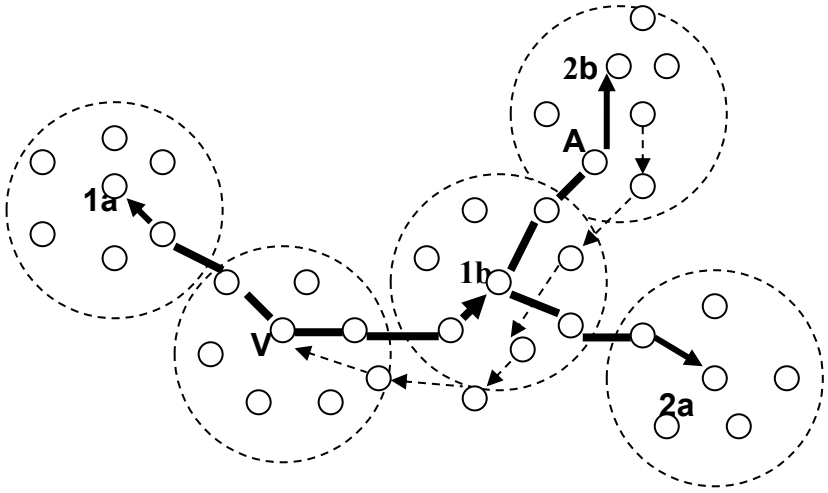

Figure 3.4.1 ***Propagation of query raised by victim V to its contacts, and query is forwarded to next higher level contacts that observed matching traffic signature within vicinity. Contacts that had lower energy value for attack signature given in query, suppress further query in that direction. Heavy line indicates the propagation of query towards attacker, whereas dotted line indicates actual path of flow of packets from attacker A to victim V. Contact centers 1a and 1b are contacted in first round, contact 1a drops further propagation of query. Contact 1b propagates to contacts 2a and 2b. Contact 2a will drop further propagation of query, and contact 2b returns the path of propagation to the victim.***

Traditional counter measures to DoS/DDoS attack are packet filtering and rate limiting. A hybrid scheme for counter measure is to apply packet filtering when abnormality matching is high. If abnormality matching is medium level, then rate limiting is used.

This scheme is suitable for particular types of DoS attacks, which tend to victimize a limited set of nodes. Any set of colluding nodes or a misbehaving contact node on the path of query will pass on the query to another node, which may not be on the stream to the attacker or will suppress the query reply to the victim.

Table 3.4: Summary of Attacker Traceback Scheme[10]

Layer	Information Provided by a layer to IDS	Information used by Layer	Action taken by IDS
MAC Layer	MAC layer Address of previous hop to be added to each packet	Routing Layer	**IDS of a victimized Node:** IDS of a victimized node can initiate a query for attacker identification by sending the attack signature, its own identity number and a sequence number to its contacts. **IDS of Nodes receiving query:** Sequence number and node identification number uniquely identify a query and if received again by intermediate nodes, then query is dropped. Intermediate node compares the received attack signature with the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

			attack signature generated by it, and computes the attack energy. If attack energy is large, then query is further passed on to a node with highest attack energy along with path traced along with the query till there is no more updation of the path attached or the query reaches an end of network (it reaches the attacker node).

3.5 Scheme proposed by Jim Parker, Anand Patwardhan, Anupam Joshi

In this scheme, the authors suggest that intrusion might be taking place by an intelligent attacker at more than one layer simultaneously. Thus detection at one layer may not suffice in identifying an attacker. Authors showed by simulation that packet dropping at routing layer and/or excessive RTS packet generation (demanding excessive bandwidth) at MAC layer simultaneously could reduce the throughput of the network drastically[12].

Table 3.5: Cross-layer Analysis for Detecting Wireless Misbehavior Scheme[12]

Layer	Information Provided by a layer to IDS	Information used by Layer	Action taken by IDS
MAC Layer	Number of RTS packets exceeding threshold during any 5 second interval		IDS (observer) nodes check if a node is requesting bandwidth more than a threshold by generating excessive RTS packets, then raise an alarm. Do post processing on the alarm to ensure that it is a true positive (malicious node). Else, if packet dropping is there but less than threshold and MAC layer also reports RTS attacks just below the threshold level, then raise an alarm for possible intrusion (suspicious node).
Routing Layer	Packet Drop		IDS node(s) check if packet dropping is more than a threshold then raise an alarm. Do post processing on the alarm to ensure that it is a true positive (malicious node). Else, if packet dropping is there (but less than threshold) and MAC layer also reports RTS attacks just below the threshold level, then raise an alarm for possible intrusion (suspicious node).

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

4. Anomaly-based Intrusion Detection Schemes:

4.1 Scheme proposed by Yu Liu, Yang Li, Hong Man

This is a rule-based based information mining peculiarity location method to identify MAC and routing layer attack on specially appointed systems. When all is said in done, peculiarity identification methods are inclined to high bogus positive rates, and require sizable computational limit and subsequently vitality utilization. In this plan a rule-based based information mining strategy, Apriori algorithm, is utilized to discover affiliation designs (rules) from review information. Since the calculation creates an enormous number of rules, these are additionally pruned by utilizing maximal successive itemset (MFI) standards[13].

A restricted set of features from routing and MAC layers is selected in[14] as given below:

Feature	**Value Space**
Flow direction (Dir)	SEND, RECV, DROP
Send address (SA)	SA_i , $\forall i \in$ node set S
Destination address (DA)	DA_i , $\forall i \in$ node set S
MACPktType	RTS, CTS, DATA, ACK
RoutingPktType (applies to MAC DATA frame only).	routingDataPkt, routingCtrlPkt

Simulation for four attacks against the network layer, namely, flooding, blackhole, sleep deprivation, packet dropping was carried on. In other words, IDS developed was focusing on detecting traffic-related attacks. The IDS system developed was effective in localizing the attacks within one hope perimeter[8]. False positive rate was reduced through the IDS decision module, where intelligence gathered from neigh boring nodes was used to make a collaborative decision and the Bayesian network is used to assess multip le sources of attack.
A comparison with [8] shows that when feature set pertains only to MAC layer (and a broader set of features of interest were considered for MAC layer alone like NAV, XmitTrafficRate, RecvTrafficRate, ReXmitRTS and ReXmitDATA), then the detection rate was lower for each of blackhole, deprivation and packet dropping attacks[15].

5. Summary of Cross-layer Information Exchanged between Layers

As suggested in [6], what information the layers should exchange amongst themselves, is still not fully developed. Here below we present a summary of cross-layer information exchanged amongst layers and the purpose for such information used in the papers described above.

Communicating Layers	Information passed on to receiving layer	In paper (reference number)
MAC layer to Routing Layer	1. Collision & Interference info so that routing layer does not selects routes through such links.	1. Svetlana Radosavac et al.[9]
	2. Buffer space available at link layer; node to accept a RREQ only if sufficient number of buffers at link layer are available.	2. Geethapriya et al.[5]
	3. MAC address of previous hop to be paired with so that node sending a large number of messages to	3. Yongjin Kim et al. [10]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 1, 2021, Pages. 09 - 20
Received 15 December 2020; Accepted 05 January 2021.

	victim node can be traced back. 4. Both MAC and routing layers share information such that only bi-directional links are used as required in IEEE 802.11 protocol.	4. Two papers: a. Svetlana Radosavac et al. [9] b. Jarmo V.E. Molsa[8]
TCP layer to Application layer	Acknowledgement of TCP layer shared with application layer so that application does not sends time-sensitive data to TCP layer when previous messages have not been cleared.	1. Jarmo V.E. Molsa[8]
Physical layer to routing layer	Low energy level for transmission of messages by a node. This node should broadcast a "low energy message" to its neighbors.	Geethapriya et al.[5]

6. Suggestions for Further Work:

A good cross-layer IDS should have the following characteristics:

1. **Low Overhead:** Time required for monitoring activities should be a small percentage so that nodes utilize most of their time in normal operations.
2. **Low false positives:** Number of times a good node is declared, as a bad node should be very small.
3. **Low true negatives:** Number of times a bad node is not detected by IDS should be very small.
4. **Low detection time:** Whatever may be the overall architecture of the system (hierarchical, cooperative, and distributed and so on), a bad node must be detected fast and appropriate response should be generated for it.
5. Should cater to a large variety of attacks. No known attack should go undetected and it should be able to detect any unknown attack.
6. Should be possible to cater to large variety of protocols used at different layers of protocol stack[16].

The techniques discussed in sections 3 and 4 above, use cross-layer approach for detecting intrusion at more than one layer. Attacks, which have not been covered in the said techniques, need to be detected either by extension of these schemes, or by developing other techniques. Detection of attacks may be done either by rule-based or by anomaly-based or specification-based techniques. Moreover, existing schemes may also be improved by better algorithm for detecting these attacks by cross-layer approach or otherwise. A complete IDS developed by using such techniques organized in a suitable architecture needs to be evaluated by above said parameters.

References:

[1] B. Subba, S. Biswas, and S. Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," *Eng. Sci. Technol. an Int. J.*, vol. 19, no. 2, pp. 782–799, 2016, doi: https://doi.org/10.1016/j.jestch.2015.11.001.

[2] Y. Yamao, Y. Kida, and Y. Kadowaki, "Cross-Layer Multi-Hopping Scheme for Efficient and Reliable Transmission in Fading Environment," in *2010 IEEE 72nd Vehicular Technology*

Conference - Fall, 2010, pp. 1–5.

[3] I. Martinez and J. Altuna, "A cross-layer design for ad hoc wireless networks with smart antennas and QoS support," in *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No.04TH8754)*, 2004, vol. 1, pp. 589-593 Vol.1.

[4] A. Anand, V. K. Sihag, and S. N. Gupta, "Wavelength conversion and deflection routing in all-optical packet-switched networks through contention resolution: a survey," in *{CUBE} International {IT} Conference & Exhibition, {CUBE} '12, Pune, India - September 03 - 06, 2012*, 2012, pp. 155–159, doi: 10.1145/2381716.2381747.

[5] G. Thamilarasu, A. Balasubramanian, S. Mishra, and R. Sridhar, "A cross-layer based intrusion detection approach for wireless ad hoc networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, 2005, pp. 7 pp. – 861.

[6] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "Cross layer-based intrusion detection based on network behavior for IoT," in *2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*, 2018, pp. 1–4.

[7] N. K. Trivedi and M. C. Trivedi, "An algorithmic digital audio watermarking in perceptual domain using direct sequence spread spectrum," 2014, doi: 10.1109/CSNT.2014.167.

[8] Jarmo V. E. Mols, "CROSS-LAYER DESIGNS FOR MITIGATING RANGE ATTACKS IN AD HOC NETWORKS," in *© 2006 International Association of Science and Technology for Development (IASTED). Reprinted with permission from Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Networks, Innsbruck, Austria, Feb. 2006, pp. 6*, 2009, pp. 286–287.

[9] S. Radosavac, N. Benammar, and J. S. Baras, "Cross-layer attacks in wireless ad hoc networks," 2004.

[10] Y. Kim and A. Helmy, "CATCH: A protocol framework for cross-layer attacker traceback in mobile multi-hop networks," *Ad Hoc Networks*, vol. 8, no. 2, pp. 193–213, 2010, doi: https://doi.org/10.1016/j.adhoc.2009.07.002.

[11] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," *J. Comput. Networks Commun.*, vol. 2019, p. 1283472, 2019, doi: 10.1155/2019/1283472.

[12] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis, and Y. Yesha, "Threshold-based intrusion detection in ad hoc networks and secure {AODV}," *Ad Hoc Networks*, vol. 6, no. 4, pp. 578–599, 2008, doi: 10.1016/j.adhoc.2007.05.001.

[13] Yu Liu, Yang Li, and Hong Man, "MAC layer anomaly detection in ad hoc networks," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 402–409.

[14] M. C. Trivedi and N. K. Trivedi, "Audio masking for watermark embedding under time domain audio signals," 2014, doi: 10.1109/CICN.2014.166.

[15] Y. Liu, Y. Li, H. Man, and W. Jiang, "A Hybrid Data Mining Anomaly Detection Technique in Ad Hoc Networks," *Int. J. Wire. Mob. Comput.*, vol. 2, no. 1, pp. 37–46, May 2007, doi: 10.1504/IJWMC.2007.013794.

[16] R. Tomar, H. Kumar, A. Dumka, and A. Anand, "Traffic management in MPLS network using GNS simulator using class for different services," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015, pp. 1066–1068.