Cross-layer Planes Framework for Detection of Malicious Nodes in WSN

Devaraju B. M., Raju G. T.

Abstract*: *Cross-layer planes design is relatively new security approach for future technological era in which different parameters are analyzed across protocols stack, so that the internet connected exchange their information with utmost security. The traditional existing approaches operates at single layer security and across few cross layers on TCP/IP model. Hence intruder can monitor loop holes on victim nodes in Wireless Sensor Network (WSN), which is serious issue for sensitive data. For example, Intrusion Detection System (IDS) operates on network layer and identifies routing attacks, but it does not react to physical layer, MAC layer and transport layers anomalies. Cross-layer design among few layers can monitor and detect some intrusions but this consumes more energy at node and node will become inactive early in the network. Hence, in this article, we are proposing Cross-layer Planes Framework for Detecting Malicious Activities (CPFDMA) at different layers is proposed to secure the WSN as viable security framework is based on the Cross-layer planes which interact attributes in different layers of the protocol stack and monitor & analyze anomaly patterns, notifying them to avoid their malicious activities from the network.

Keywords: WSN, Cross-layer Framework, Malicious Activities.

I. INTRODUCTION

In WSN, sensors are scattered and inter-connected for communication on designated area. Sensor nodes are deployed in areas where no human interaction is possible or very difficult. The sensor device has capability of sensing many parameters like, temperature, pressure, humidity so on, from the surrounding circumstances of the application [1]. WSNs are used to collect sensitive information in designated area, but network would become susceptible to various threats and attacks at different layers of the protocol stack or attack on nodes [2]. There will be a need to improve defense or security, that will advantageous to the successful deployment of nodes in wireless sensor networks. Moreover, WSNs have limited in computation power, bandwidth, memory capacity and energy. WSN faces severe security problems due to communication in wireless media, because nodes are deployed in open hostile area. So security is most important aspects among nodes communication.

The attacker can disrupt the security parameters by launching attacks at different layers or node of the WSN. An intrusion is any sort of unauthorized activities carried out by attacker and which are damage network resources or on sensor nodes. The massive research conducted by the researchers to provide security solutions for various attacks in the WSNs so far was based on the layered approach [3][4]. In this survey, we put emphasis on the layered approaches have noticeable limitations as the redundancy and inflexibility of the security solutions, which made the layers security solutions often inefficient and inadequate. It remained us, beneficial to construct the security approach for the WSNs based on cross-layer and cross-layer planes interaction between all the parameters in different layers of the protocol stack. Due to the energy, memory and computational power limitations, designing appropriate detection and prevention mechanism for WSN is a challenging task.

In this article, CPFDMA is proposed to detect such unauthorized or malicious activities and is widely used for securing WSNs. This framework consists of Cross-layer Intelligent Monitoring Agent (IMA) which ensures cross-layer information exchange amongst physical, MAC, and network layer and management planes in WSN. The primary functions of IMA are to monitor users' activities and network behavior at different layers parameters. IMA can detect an intrusion and raise an alarm for appropriate action by the admin or automation solution by IMA. IMA is used for local events monitoring as well as neighbors monitoring based on location information, power analysis and node tasks. This module mostly monitors traffic patterns, internal events, and resource utilization. IMA can detect multi-layer security attacks and anomaly activities. Cross-layer Data Unit (CDU) collects and represents data from layers of TCP/IP protocol stack.

Analysis and Detection Unit (ADU) is the main unit which is implemented based on modeling and machine learning techniques. The network operations, behavior of the node/s and activities/task are analyzed and decisions are taken to proclaim them as malicious or not. Alarm Unit (AU) is a response generating parametric values, which raises an alarm in case of detection of a malicious activities or intrusions. The architecture or framework we have proposed has good detection rate. It is noted that IDSs systems are passive in nature and can only detect intrusions. But they could not take any preventive action. They can produce an alarm. It is then the administrator's needs to take preventive measurements against the attack.

Revised Manuscript Received on December 15, 2019.
***** Correspondence Author

Devaraju B M , Assistant Professor, CSE, RNS Institute Of Technology, Bengaluru, India.

G T Raju, Vice Principal, Professor and Head of CSE, RNS Institute Of Technology, Bengaluru, India.

But our proposed system is to take few preventive measures on active malicious nodes for avoiding them in interaction with normal nodes.

II. RELATED WORK

In Wireless Sensor Network, the protocol stack communicates with complex algorithms for data transfer from one node to other node which resulting problem with implementation, debugging and upgradations. These are inefficient way implementation for maintaining QoS and avoid malicious activities in network. Existing cross-layer design is alternative to improve QoS, but it has complex communication process, because data has encapsulated in the protocol stack and this approach has least significant on security issues. The main idea behind cross-layer planes framework design is to improve QoS and increase network performance through detecting and avoiding malicious activities in WSN by using cross layer management plane layers parameters list.

Recently several researchers have been done work on cross-layer design, architectures framework, instruction detection and prevention on network attacks. Melodia et al. narrate the literature survey on cross-layer protocols design and classifications for WSN [5]. Wang et al propose a cross-layer design approach for lowering energy consumption and increasing WSN lifetime of many source nodes and sink node with different parameters [6]. The authors are proposed existing cross-layer methods are sharing information through management and non-management planes layers [7][8]. Several researchers are finding ways to integrate cross-layers and design approaches into wireless communications for purpose of allocating resources across the mobile nodes/phones, scheduling resources for good throughput and maintain better QoS for mobile phones/nodes applications [9]. The sensor network poses unique security challenges and layered and cross-layered shown to be adequate schemes, so that lot of research work to be carried out on vulnerability and network performance to avoid attacks. Cross layered interactions used to detect attacks and provide intrusion tolerance for network survivability [10].

Ant System algorithm to avoid DoS in network using cross-layered routing protocol proposed in [11] which is extended to other security anomalies pattern predictions. In distributed network, detect of intrusion through Genetic algorithm, Ant colony algorithm, and Ani-Phase Synchronization algorithms implemented at different layer in WSN on pattern of cross layer interaction [12]. The author proposed Cross-layer design in WSN for reducing energy consumption thereby improving network lifetime by data aggregation. The data aggregation has been done at sink node with constrained routing algorithms, thereby increasing QoS in the network [13]. Xu, N et al., proposed Energy efficient cross-layer security framework and cluster based secure key scheme for high energy efficient, secure communication and attack resistance. The work has been carried out based on analyzed threads and characteristics of WSN [14]. Gandhimathi et al., The cross-layer features correlated with neighbors and pattern to detect attacks in WSN. Agent based approach used to detect attacks like Sinkhole, Wormhole and Sybil attacks [15][17].

Pugliese et al., proposed model for detection which is fully distributed with dynamic hierarchical architecture and security functions are executed by node. The complexity is reduced due to clustered tree topology which avoids loop checks and polling among neighbor nodes [16]. The author proposed cross layered approach with distributed beamforming technique to boosting the Base Station secrecy, so that which limits secrecy related control messages in WSN in turn results reduces energy overhead [18]. The QoS is an important requirement in WSN to achieve node must maintain feasible route selection process. Thereby large latency and malicious packet drop rate are serious to the network performance. By adopting cross-layer approach path selection in a router and router has features like, higher throughput, lesser delay and minimum loss rate [19]. A framework for security analysis through cross-layer design in Avionics inter communication systems and features associated to 5G technology have been presented using low latency and high reliability [20].

III. CROSS-LAYER PLANES FRAMEWORK FOR DETECTING MALICIOUS ACTIVITIES (CPFDMA)

Security attacks in WSNs are classified into two types. One is active attack and other one is passive attack. Passive attacks use significant information from the wireless sensor network; they do not harmful to the network resources or networks. But active attack used to temper, misdirect and drop the packets. The distinctive characteristics of wireless sensor networks wireless media, contention-based media access, multi-hop communication, designed decentralized architecture and random deployment of nodes in specific area, such networks make more in vulnerable at all layers in protocol stack. The active attack will be classified into malicious activity and anomaly attacks. The malicious attacks are known attacks which are defined as patterns of activities. The anomaly attack generates new signatures of attack. Predicting anomaly attacks are more false positive than malicious attacks.

The security of a network is to be implement in all the layers TCP/IP protocol stack and to implement security would be more complex in process, inefficient and inadequate. So, we are proposing Cross-layer planes Framework for Detecting Malicious Activities. We believe that the cross-layer planes framework design is a unique applicant to provide a better security solution for the network.

A Cross-layer Planes Framework for Detecting Malicious Activities (CPFDMA) at different layers by aggregating parameters is shown in Fig. 1. The parameters observed from different layers will consolidated at management planes and select set of parameters to create Audit parameter list. The audit parameters are helpful for detecting threats in the network by node source address. These parameters have been feeding into the Intelligent Monitoring Agent module. The agent module integration of parameters interface, Cross-layer Data Unit (CDU), Analysis Detection Unit (ADU), Alarm Unit (AU) and Machine Learning module.

IMA is used for local events monitoring as well as neighbors monitoring based on location information, power analysis and node tasks. This framework regularly monitors traffic patterns, internal events, and resource utilization. IMA can detect multi-layer security attacks and anomaly activities.

Cross-layer Data Unit (CDU) collects and represents data/parameters from all layers. Analysis and Detection Unit (ADU) is the main component which is based on modeling. This model will have to suggest aggregated parameters based on relativity with parameter attributes.

Machine learning module has been fetching data through CDU and ADU for analyzing network operations, behaviors pattern values and attributes values then decisions are taken to declare/predict them as malicious or not. Also, ML algorithms predict type of malicious attacks. Fig. 2 shows the architecture of CPFDMA. Table- I give different TCP/IP Layers attacks and different parameters/attributes. Table II shows the different WSN protocol stack Layers, Attacks parameters/attributes.

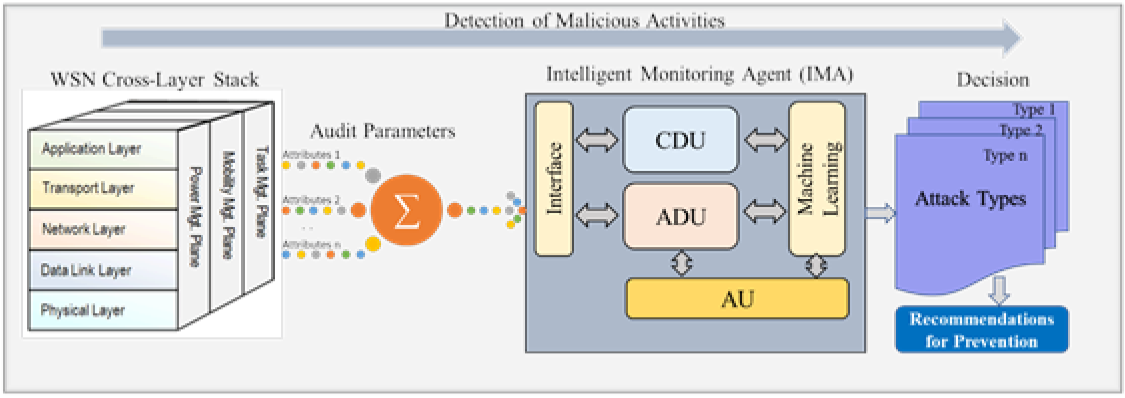

Fig 1: Cross-layer Framework for Detection and Prevention of Malicious activities in WSN

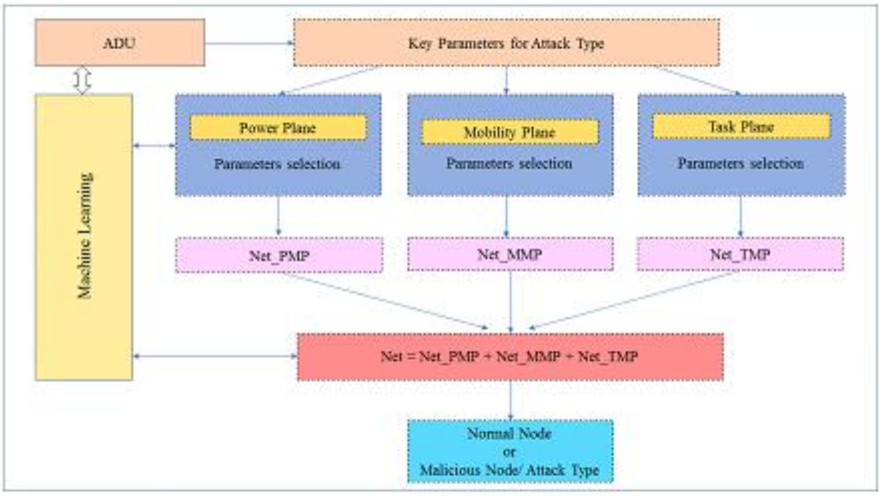

Fig 2. CPFDMA for WSN

Table II: WSN protocol stack Layers, Attacks parameters/attributes

TCP/IP	Power Management layer Parameters	Mobility Management layer Parameters	Task Management layer Parameters
Applic ation Layer	Node ID, Data type, Code size, Data size, Energy level, Packet dropping rate, Packet sending rate,	Node ID, Log files, Login credentials, Node location,	Node ID, Data type, Log files, Pattern matching, semantics data analysis,
Transport Layer	RST Packet, SYN+ACK messages, Packet Response Rate, buffer size w.r.t time, Bandwidth of channel, Bandwidth of channel, Memory, SYN-ACK packets, RST/FIN, ICMP echo request count,	Avg response delay, Authenticate the validity of Random number, Shared secret key, Session time, Bandwidth of channel, RST/FIN, ICMP echo request count.	Session ID, SYN number, Session Keys, Time out Time stamp, Packet Response Rate, Port number, Authenticate Type, Authenticate the validity , Shared secret key, Session time, Port status message, Sequence no., Packet type

Network Layer	IP address, time stamp lifetime, RREQ, RREP, packet delivery ratio, Packet arrival process & time, Signal power/ received signal strength, Transmission power, number of nodes, hop count, Delay, Throughput, Packet receiving rate, Packet dropping rate,.	Node IDs, IP address, Keys and Validation, Sequence no., time stamp lifetime, RREQ, RREP, Packet relay, Location, no. of nodes, hop count, RTS, Packet forward rate, Forward delay time.	IP address, Sequence no., Packer sending rate, Keys and Validation
Data link Layer	Neighbors count, Power, RSSI, Number of packets delivery ratio, collision rate, RTS/CTS, BER, Buffer size, RTS rate	Neighbors count, RTS/CTS, MAC address, Neighbors count, Node count	CRC, CSMA/CA parameters
Physical Layer	Collision rate, RSSI, Duty cycle, RTS count, Energy level and power calculation for transmission, Baud rate, Number of interfaces, Duty cycle	Node ID, Location, channel state information (CSMA/CA), relay selection, Abnormal environmental conditions	Number of interfaces, Decapsulation,

Table- I: TCP/IP Layers attacks and different parameters/attributes

TCP/ IP	Attacks	Attributes
Application Layer	DoS	Data type, user commands, login credentials, code size, log files, Node ID, Application priority, packet loss rate *P, Energy consumption E and the Distance D,*
	Data corruption	Node ID, Login credentials, Pattern matching, semantics data analysis, outliers detection
	Node compromise	Data accuracy, Data size, KDS, Pattern matching, Energy level, location of the node, Packet drop rate, Packet send rate, Brute force.
	Malicious code attack/ malware attack/ Node malfunctioning	Intrusion semantics, Pattern matching, physical address location, JMP and LOOP instructions. IN and OUT instructions
Transport Layer	Session hijacking, SYN flooding, DoS	Session ID, SYN number, Session Keys, MTU/MRU, RST Packet, TCP Header, SYN+ACK messages, Time out Time stamp, Sequence no, Avg response delay, Packet Response Rate, Port number, buffer size w.r.t time. TCP header checksum, TCP header options, Congestion window, RTT estimation, Receiver window,
	De-synchronization (illegal Control Flags)	Authenticate Type, Authenticate the validity of Random number, Shared secret key, Session time,
	Packet injection attack	Bandwidth of channel, Packet information, Port status message,
	Flooding Attack, DoS (wastage of memory)	Sequence no, Packet type, Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth, TCP SYN , TCP SYN-ACK, ACK & PUSH ACK, RST/FIN, ICMP echo request count,
Network Layer	Black hole Attack	IP address, Sequence no. time stamp lifetime, RREQ, RREP, packet delivery ratio, Packet dropping rate, Packet arrival process, Location
	Selective forward Attack	IP address, Sequence no. time stamp lifetime, RREQ, RREP, Signal power/ RSSI, Transmission power,
	Sybil Attack (node carries different identities)	Packer sending rate, Node IDs, CA details, Resource tests, Location, RSSI, Keys and Validation
	Worm hole (tunneling for long distance)	One hop node, Node ID, high-power source, high bandwidth channel, Packet Encapsulation, Out -of -band Channel, High power Transmission Capability, Packet relay, Location, Interface number. RSSI, hop count, RREQ, RREP, RTT, Buffer v/s data transmission. Signal power/ received signal strength, Transmission power/packet sending power
	Node replication	Location, Node ID, IP Address, Data type, Security Keys, no. of nodes, hop count, ICMP message, IP header options,
	Sinkhole Attack	link quality, hop count, node ID, RREQ (Route request), RREP (Route Reply), Routing metric. No. Packets sent & received, Packet Delivery Ratio (PDR), Delay, Throughput, Packet receiving rate. Hop count, Packet forward rate, RSSI, Packet arrival process
	Spoofed, Altered, replayed	IP address, data type, hop count, RTS
	Ack spoofing	IP address, neighboring count,
	Hello flood attack	Packet dropping rate, Packet arrival process, Packet forward rate, Forward delay time
Data link Layer	Traffic analysis, monitoring,	Neighbors count, Power, RSSI, Number of packets delivery ratio, collision rate
	Node Outage, Collision	Collision rate, RTS/CTS, CRC, Power
	Disruption MAC	MAC address,
	Exhaustion	BER, Collision rate, Buffer size, RTS rate, Neighbors count, Node count, RED (average queue length), Agent (ACKs list block), Length of *K* packets, queuing delay,

Physical Layer	Signal Jamming	Collision rate, RSSI, Duty cycle, RTS count, Location, Number of frequencies at same interfaces, Signal power/ RSSI/received signal strength, Transmission power/packet sending, Good/Bad threshold (channel fading)
	Interceptions, Eavesdropping	RSSI, Energy level and power calculation for transmission, Node ID, Location, channel state information (CSMA/CA), relay selection,
	Physical Tampering / Node capture Attack	RSSI, Baud rate, BER, Power consumption rate, Beacon signal- RST, Location, Sensing reading report rate, Abnormal environmental conditions, Load estimation (intra-cell interference, BS transmitpower) Number of interfaces, Data remanence, Decapsulation, clock glitches, CRC, Duty cycle

A. Parameters at different layers

Packet Collision Ratio (PCR): PCR calculated when two or more sensor nodes send packets at same instant are collide through shared media. Collide packets are discarded and retransmitted and this is handled by CSMA/CA in MAC layer. LEACH protocol has been proposed to avoid collision in channel, but adversary nodes can attack on schedule protocols. The high collision rate indicates the existence of attacks.

Packet Delivery Waiting Time (PDWT): The packets have to wait for shared media in CSMA protocol and waiting time is having threshold level. Attacks can be identified if value of threshold increases variably.

RTS Packets Rate (RPR): To avoid collision, MAC protocol implemented with RTS/CTS signals. If attacker sends larger number requests to send packets, then receiver exhausted and energy will be drained.

Neighbor Count (NC): In larger sensor network, node must be uses multi-hop routing for communication. Every node must maintain routing table. New node could be added to the network and removed frequently, so energy could be exhausted over the time from this change we could identify some attacks. Example Sybil attack.

Routing Cost (RC): In larger network, every node maintains a routing table to route the packets along with its cost or latency of the route. In sinkhole attack malicious node has send bogus route information to attract more packets. Keep monitoring route cost, latency and analyze them to detect attacks.

Power Consumption Rate (PCR): all sensor nodes have designed with constrained limited power. The power consumption by processing unit, sensing unit, radio communication and with other processing components in node. But protocol has designed to save energy. SPIN routing protocol access the current state of battery and runs suitable protocol. But DoS attack aim to drain the energy by increases collision or sending more RTS packets.

Sensing Reading Report Rate (SRRR): Sensors having sensing function to sense the application parameter at different reading rate. Some sensors reading periodically with fixed rate and some sensor answered only for the queries. Malicious node could frequently query to exhaust the victim energy.

Distribution of Packet Type (DPT): In WSN packets/sensing data are transmitted in wireless such as sensing data, route updates, and query/commands. The intension of WSN is to sense certain interesting information.

Packet Received Signal Strength (PRSS): The Received Signal Strength measures electromagnetic energy between transmitter and receiver. If RSS is greater than threshold value is receiver sensitivity. The estimated distance can be calculated by RSS and propagation model. If node receiver signal decreases continuously indicate attacks on node and RSS increases, then node ID could stolen by potent malicious node.

Sensing Data Arrival Rate (SDAR): Sensor has to sense data on basis of some particular event occurs and on regular interval. If either missing data sensed or unexpected sensed data received will identifies abnormality or malicious node.

Sensing Reading Value Changing Ratio (SRVC): If sensing reading data changes beyond its normal range, then there could be a malicious activity.

Packet Drop Ratio (PDR): In larger network, communication has in multi-hop routing. Nodes must receive and forward data frequently at deserved rate. The attack node could drop packets or selectively forwarding some packets. Here subverted node forwarding rate, receiving rate and dropping will be highly varied compared with normal node.

Packet Retransmission Rate (PRR): The packets will be retransmitted when data transmission failed, or packets are corrupted. If node is compromised, multiple time request for packets to exhaust the victim energy. Abnormal retransmission rate could able to detect attacks.

Table-I describes TCP/IP layers, different attacks in every layer and each layer attacks parameters/attributes are listed. In Table-II, we have classified aggregated attacks' attributes into three management plane layers. These are the audit attributes/parameters that have been fed into IMA module interface for further process of CPFDMA. Algorithm is given below.

```
Generic Algorithm: CPFDMA
Step 1: Set quality Audit parameter $N$
Step 2: $N$ value range [$Nmin$, $Nmax$].
Step 3: Calculate average N values with given interval of time $[t]$
Step 4: $N$ random variable mean value is assigned
          {$N$ gives the best performance value under
           current network conditions}
Step 5: Calculate Standard Deviation ($\sigma$) for $N$ and stored
Step 6: Declare it as an attacker node /malicious activities
```

B. Types of Attacks on Networked Protocol Stack

a. *Physical Layer Attacks*: Spread spectrum communication defenses signal jamming [21]. Different authors proposes tamper-proofing design for protect from selecting medium, selection of frequency, carrier frequency at media, signal modulation-demodulation and data encryption. Also, it must deal with the design of the underlying hardware and various electrical and mechanical interfaces.

b. *Data Link Layer Attack*: the objective of Medium Access Control layer is to, fairly and efficiently shared resources among multiple nodes in WSN to achieve good throughput, packet delivery and latency. Cipher Block Chaining encryption scheme using Advance Encryption Standard algorithm and Sensor information exchange via negotiation and broadcasting authentication protocol used in µ TESLA[22][23][24]

c. *Network Layer Attack*: Whenever route request receives from neighbors sends replay from malicious node to attract the traffic and drop them all i.e., Blackhole Attack [25]. The compromised node setup high speed tunnel with malicious node in other networked and all packets through tunnel [26]. Hop count technique and Round-Trip Time (RTT) [18] implemented to avoid them.

Nodes can monitor the behavior of neighboring nodes and find them [19][20]. A node illegitimately creates multiple IDs and violates rules. To detect Sybil attack, malicious node may send same RSSI beacon with different IDs [27], suspect the node and locate the attacked area, using network flow graph, find massage digest using MD5/SHA1. Hacker spoof link layer ACK and overhead by ACK packets on the network [28]

d. *Transport Layer Attacks*: Adversary node sends many requests to victim for connection and victim must allocate memory for store connection state information, but this overhead less compare to flooding. Protocols are connectionless therefore naturally stateless, but they are not providing proper transport level services for network. To overcome this client must solve puzzle [29] before receiving a connection with server node.

e. *Application Layer*: Majority of attacks on networks recently because of there are more complex applications have been running on node. Malware are very dangerous on hardware part of the node. Using SQL and Cross site scripting attacker can easily establish malicious activity on nodes. DDoS attacks on application layer solved by many feature [30].

Power Management Plane: There is a need to manage and optimize power consumption on the node. This can be done through avoiding redundant data in network, setting the node active only during data processing and transmitting and receiving. Machine learning algorithms can be used to analyze data pattern in order to reduce the power consumption and avoid malicious activities.

Mobility management plane: Managing the mobility or routing of the node in the clustered network. The node can be localized properly and accurately in network that can result in saving energy and avoid malicious activities. Deep learning algorithms can be used to analyses the mobility pattern in order to avoid malicious activity in the network.

Task Management plane: Manages the process at node in order to perform the operations depending on application requirements. The node can share and schedule resources efficiently in the network and coordinate all the plane tasks in this layer for avoiding malicious activities.

The existing proposed security solutions cross-layers approaches are less compatible to all existing topologies for WSNs. Here, we present the most motivating frameworks for network topologies that is, Parametrical cluster formation. We predict that the single layer or few cross-layer security solutions is often inefficient and inadequate in WSNs. Still, there is a beneficial to construct the security through cross-layer planes framework approach for the WSNs at different layers of the protocol stack. This work objective is to break with the conventional layering directions. We have propose novel cross-layer planes based comprehensive CFDMA for parametrical clusters in wireless sensor networks.

In the proposed framework, important set of parameters are monitored at different l layers protocol and the Net values of sensor nodes calculated and find the standard deviations value of parameters. Then compare the Net value and pre-calculated threshold. The decision are made to whether the sensor node is compromised or not and attack type. The Net values of sensor nodes gives more accurately by considering the deviations of parameters of multiple layers. Henceforth our proposed scheme is effective for detecting attacks in WSN.

IV. RESULTS AND DISCUSSIONS

Fig. 3 presents different kinds of most dangerous attacks on network, as per the survey made by McAfee Labs Threats Report in August 2019. More number of malware and vulnerability attacks observed from the statistical data

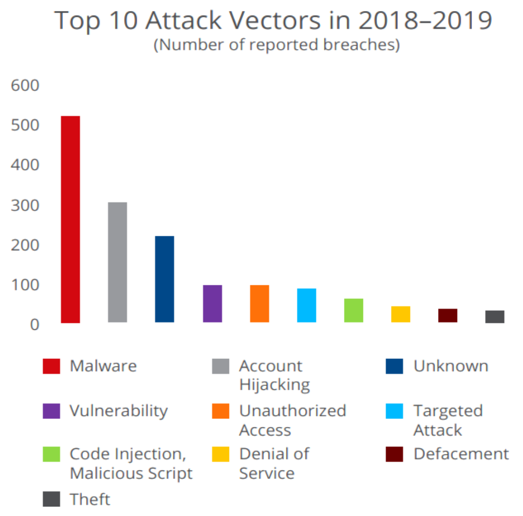

Fig 3: Top 10 types of attacks in the year 2018-2019

In Fig. 4, new IoT malware attack rate at every is presented and it increases every quarter year. IoT devices are largely investigate into human life, so malicious activities also keep increases.

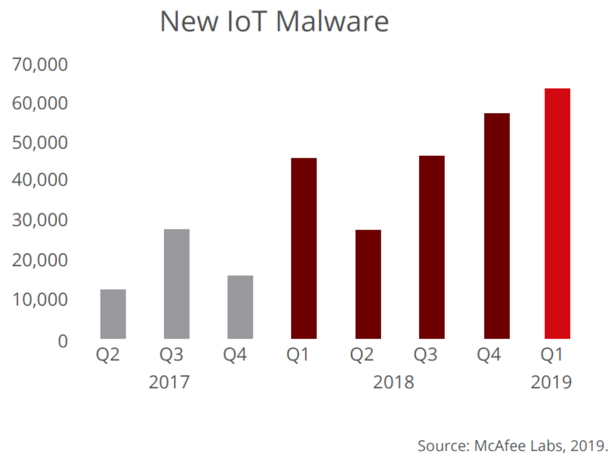

Fig 4: New IoT malwares rate at every year

Fig. 5 presents the most targeted industries in global level. Highest attacks in the field of healthcare, individual attack, public and financial sectors

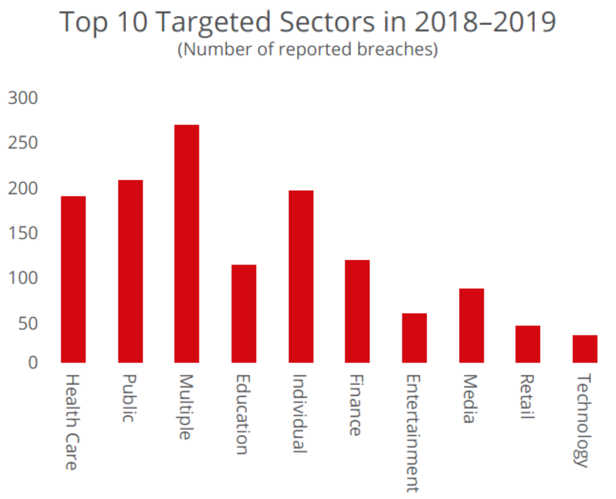

Fig 5: Top Targeted industry sector in 2018-2019

V. CONCLUSION

In this paper, the network security framework for WSNs, CPFDMA has been proposed and presented as an effective security solution for various applications in WSNs, which in turn results to saving of energy in large extent. Also this framework results, distance aware and parametric clustering, secure routing based on interplaying parameters among all planes layers of the protocol stack in WSNs. As it is vital to provide security services to entire wireless sensors in network. The proposed framework may give new directions towards providing securing for communications and extending the lifetime of the entire wireless sensor networks.

ACKNOWLEDGMENT

Authors thank the management of RNS Institute of Technology, Bengaluru for their unconditional support and cooperation.

REFERENCES

1. Borges, L. M., Velez, F. J., Lebres, A. S. “Survey on the Characterization and Classification of Wireless Sensor Network Applications”. IEEE Communications Surveys & Tutorials, 2014, pp. 1860–1890.
2. Patle, A., Gupta, N. “Vulnerabilities, attack effect and different security scheme in WSN: A survey”. 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016.
3. Gandhimathi, L., Murugaboopathi, G. “Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent”. International Conference on Information Communication and Embedded Systems (ICICES), 2016.
4. Mingbo Xiao, Xudong Wang, Guangsong Yang. “Cross-Layer Design for the Security of Wireless Sensor Networks”. 6th World Congress on Intelligent Control and Automation, 2006.
5. T. Melodia, M. C. Vuran, D. Pompili, “The State of the Art in Cross-layer Design for Wireless Sensor Networks," Proc. EuroNGI Workshops on Wireless and Mobility (Springer Lecture Notes in Computer Science 3883), 2005.
6. Akyildiz, I. F., Xudong Wang. “Cross-Layer Design in Wireless Mesh Networks”. IEEE Transactions on Vehicular Technology, 2008, 57(2), pp.1061–1076.
7. V. Srivastava, “Cross-Layer Design: A Survey and the Road Ahead” IEEE Communications, 2005.
8. F. Foukalas, V. Gazis, and N. Alonistioti, “Cross-Layer Design Proposals for Wireless Mobile Networks: A Survey and Taxonomy,” IEEE Commun. Surveys & Tutorials, 2008, pp-70-85,.
9. Foukalas, F., Gazis, V., Alonistioti, N. “Cross-layer design proposals for wireless mobile networks: A survey and taxonomy”. IEEE Communications Surveys & Tutorials, 10(1), 2008, pp.70–85
10. Mingbo Xiao, Xudong Wang, Guangsong Yang. “Cross-Layer Design for the Security of Wireless Sensor Networks”. 6th World Congress on Intelligent Control and Automation, 2006.
11. Muraleedharan, R., Osadciw, L. A. “Security: Cross Layer Protocol in Wireless Sensor Network”. Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, 2006.
12. Hortos, W. S. “Bio-inspired, cross-layer protocol design for intrusion detection and identification in wireless sensor networks”. 37th Annual IEEE Conference on Local Computer Networks, Workshops, 2012.
13. Mishra, M., Gupta, G. S., Gui, X., “A Review of and a Proposal for Cross-Layer Design for Efficient Routing and Secure Data Aggregation over WSN”. 3rd International Conference on Computational Intelligence and Networks (CINE), 2017.
14. Xu, N., Sun, Y., Huang, B.,Yu, J. “An Energy-Efficient Cross-Layer Framework for Security in Wireless Sensor Networks”. 2011 Fourth International Symposium on Knowledge Acquisition and Modeling, 2011.
15. Gandhimathi, L., Murugaboopathi, G. “Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent”. International Conference on Information Communication and Embedded Systems (ICICES), 2016.
16. Pugliese, M., Pomante, L., Santucci, F. “Agent-based scalable design of a cross-layer security framework for Wireless Sensor Networks Monitoring Applications”. International Conference on Ultra-Modern Telecommunications & Workshops, 2009.
17. Aryai, S., Binu, G. S. “Cross layer approach for detection and prevention of Sinkhole Attack using a mobile agent”. 2nd International Conference on Communication and Electronics Systems (ICCES), 2017.
18. Ward, J. R., Younis, M. “A Cross-Layer Distributed Beamforming Approach to Increase Base Station Anonymity in Wireless Sensor Networks”. IEEE Global Communications Conference (GLOBECOM), 2015.
19. Shi, P., Shi, P., Gu, C., Ge, C., Jing, Z. “QoS Aware Routing Protocol through Cross-layer Approach in Asynchronous Duty-cycled WSNs”. IEEE Access, 2019. P.1–1.
20. Samano-Robles, R. “MAC-PRY Cross-Layer Design for Secure Wireless Avionics Intra-Communications”. Eighth International Conference on Emerging Security Technologies (EST), 2019.
21. Rose, S. G. H., Jayasree, T. “A jamming detection technique for WSN using timestamp”. IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2017.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

22. Nigussie, E., Isoaho, J., Virtanen, S., Hakkala, A. “Energy-aware adaptive security management for wireless sensor networks” A World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE 15th International Symposium on, pp. 1-4, 2014.
23. Saleha Mubarak AlMheiri, Hend Saeed AlQamzi,. “Data link layer security protocols in Wireless Sensor Networks: A survey” Networking, Sensing and Control (ICNSC), 10th IEEE International Conference on, 2013, pg. 312 – 317.
24. Daud, M., Rasiah, R., George, M., Asirvatham, D., Rahman, A. F. A., Halim, A. A. “Denial of service: (DoS) Impact on sensors”. 4th International Conference on Information Management (ICIM), 2018.
25. Kumar Sandeep, Suman Sangwan, "A Survey of Black Hole Detection Techniques in WSNs", IJARCCE, vol. 4, 2015.
26. Meghdadi Majid, Suat Ozdemir, Inan Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks", IETE Technical Review, vol. 28.2, pp. 89-102, 2011.
27. James Newsome, Elaine Shi, Dawn Song, Adrian Perrig "The Sybil attack in sensor networks: analysis & defenses" IPSN'04, California, USA, April 26-27, 2004.
28. Al-Mashhadi, H. M., Abdul-Wahab, H. B., Hassan, R. F. “Secure and time efficient hash-based message authentication algorithm for wireless sensor networks”. Global Summit on Computer & Information Technology (GSCIT), 2014.
29. Saif, D., Cormier, A., Banik, S., Matrawy, A. “A Review of Recently Emerging Denial of Service Threats and Defences in the Transport Layer”. IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2018.
30. Praseed, A., Thilagam, P. S. “DDoS Attacks at the Application Layer : Challenges and Research Perspectives for Safeguarding Web Applications”. IEEE Communications Surveys & Tutorials, p-1–1, 2018.

AUTHORS PROFILE

Devaraju B M is currently working as Assistant Professor in CSE department of RNSIT, Bengaluru, affiliated to VTU. He is pursuing PhD at VTU and his research interests include WSNs, Network Security, and Cryptography.

Dr. G T Raju has received M.E. (CSE), Degree from Bangalore University in 1995 and Ph. D (CSE) from Visvesvaraya Technological University (VTU), Belagavi, Karnataka in 2008. Currently working as Vice-Principal, Professor & Head in the Department of Computer Science & Engineering , RNS Institute of Technology, Bengaluru, Karnataka – 560 098. He has 25 years of teaching and research experience. His areas of research interests include Web Mining, Semantic Web, Artificial Intelligence, Machine Learning, Knowledge Data Discovery, Internet of Things, Image Processing and Pattern Recognition. He has published 100+ research papers in reputed International Journals and conferences. He has authored 5 technical text books. He has completed two funded projects. 10+ Research Scholars have been awarded Ph. D degree under his supervision.