IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 26, No. 6, December, 2021, pp. 559-567
Journal homepage: http://iieta.org/journals/isi

Pragmatic Security-Aware Cross-Layer Design for Wireless Networks from Vampire Attacks

Battula Phijik[1*], Chakunta Venkata Guru Rao[2]

[1] Department of Informatics, Osmania University, Hyderabad 500007, Telangana, India
[2] School of Computer Science & Artificial Intelligence, SR University, Warangal 506 371, India

Corresponding Author Email: phijik@vmtw.in

https://doi.org/10.18280/isi.260606

Received: 10 October 2021
Accepted: 19 November 2021

Keywords:
cross layer design, wireless networks, vampire attack, carousal and stretch attacks

ABSTRACT

Wireless networks rely on ad hoc communication in an emergency, such as a search and rescue or military missions. WLAN, WiMAX, and Bluetooth are often used in Ad Hoc networks. Using a TCP/IP wireless network poses several challenges. Packet loss in 802.11 may be caused by noise or the network. TCP/IP connects non-adjacent layers of the network, resolving cross-layer communication technology for cross-layer communication. It regulates data transmission energy. This structure solves an issue in various ways. It is often used to improve data transfer. Currently, the OSI reference model's layers and functions are not explicitly connected. Only DCL can send multimedia data via wireless networks. The research employs CLD to improve wireless security—invasions of ad hoc networks (MANETs). The research helps secure wireless MANs (MANETs), Vampire Attack Defense (VAP) algorithms. A Secure Cross-Layer Design SCLD-AHN protocol is included. The paper contributes to controlling security attacks in wireless Mobile Ad Hoc Networks (MANET's). In MANETs effectiveness of Vampire Attack Defense (VAP) algorithms is evaluated and analyzed. It also proposes a Secure Cross-Layer Design for the ad hoc networks (SCLD-AHN) protocol.

1. INTRODUCTION

Now people are widely using the Internet. It only takes a few seconds to send a text message. Other people can upload a video when alerted in microseconds. Even though in many places, Internet connectivity is weak, but the multimedia communications required. Sensor zones need communication between drones. The multimedia server has to make rescue operations, search activities, emergency usage in battle areas and meeting rooms. In the examples provided, everyone needs a node to collaborate. The ad hoc networks of two types Static and Dynamic. In static nodes, fixed called Static-Ad-Hoc-Networks (SANET). In dynamic AdHoc networks, the mobility of nodes (active nodes) happens called the Mobile Ad Hoc Network (MANET). In MANET, an individual node acts as a system and router. It can be deployed everywhere without infrastructure networks. These features make the AdHoc network ideal for situations such as search, rescue operations, combat areas and emergency use. It also challenges the MAC layer to communicate between transport and network layers of TCP / IP reference models [1].

The MANET faces many architectural issues, such as persistent link crashes. Several routing algorithms proposed to solve these problems. Here a couple of ways to manage ad hoc network routing protocols. The first is a proactive Destination-Sequenced Distance Vector (DSDV) routing protocol. The second is the reactive Optimized Link State Routing Protocol (OLSR). DSDV is an active routing protocol that uses the destination generated array number [2, 3]. It helps to identify the old ways. The OLSR prevalent link-state routing protocol overheads with a link table. In OLSR, delay and scalability are low. Existing well-known algorithms are Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing protocols [4]. It searches for the route when needed. The primary use of a proactive routing technique is the scalability of nodes, but it leads to transmission delay. The IEEE 802.11 is standard for MAC layer and ad hoc networks, but Ethernets not ensembles in wireless environments. The IEEE 802.11 standard assumes error is minimal in wired, but in wireless links, it is very high [5].

On the other hand, two-layer security, power usage, and frequent connection breaking problems in Ad-hoc networks addressed. The Network, MAC Layers and Protocol Stack to address these issues. Issues such as power optimization and throughput improvement with energy control. Transmission of power is a significant issue in MANET for more performance. It is because it affects almost all layers. However, this requires cooperation between all layers. CLD manages to find the right resolution for optimization. The cross-layer design acts as intermediate to each layer to solve the problem [6]. The primary method of energy transfer proposed. In this case, the RTS-CTS sends the highest transmission power. The Data-ACC packets the packets to deliver the minimum required level.

The advantage of consumptive transmission control is that it optimizes power intake and increases capability. Energy requirements disturb layers transmissions. However, physical, MAC, and network layers play an important role in enhancing performance. Srivastava et al. [7] proposed the mechanism for interactions between the network, MAC and physical layers for cross-layer design. In wireless sensor networks, (WSN) power transmission utilized to solve energy issues in VANETs,

and MANETs. In VANET, the transmission of security communications required to send the maximum number of vehicles. However, this requires further expansion of power and increases the controversy. Power consumption is the highest in sensor networks. However, this can lead to dis-connectivity on the network. De Cicco and Mascolo [8] proposed an algorithm that minimizes connectivity maintenance, energy consumption. The significant problems in cellular networks are power, age, and throughput, verified for Code Division Multiple Access.

Additionally, Cognitive Radio (IEEE 802.22) permits unlicensed operators to make better usage of the licensed networks. The primary issue with 802.22 is that it reduces secondary user engagement. Based on the non-cooperative game theory, the dynamic bandwidth allocation performed.

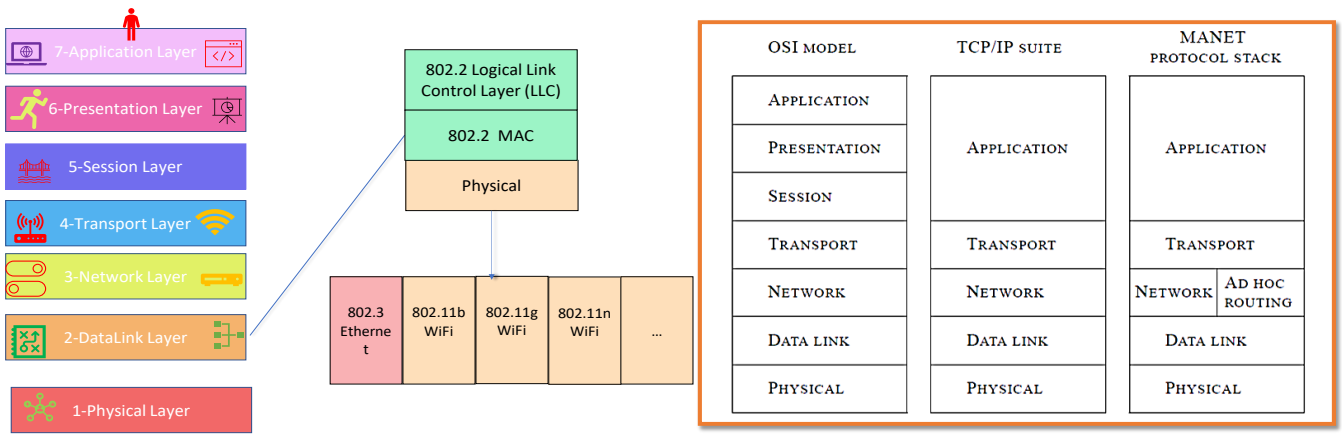
2. PRELIMINARIES

The wireless networks depend on the bandwidth to cover the topographical area range. The transmission range depends on data optical signals and routing wavelengths and the proliferation of wireless technologies, sensor networks, personal, body area networks (PAN, BAN), infrastructure-less networks vast, wide, (VAN's, WANs) and MANETs. Every wireless protocol creates issues and needs precise resolutions. Still, it solved using cross-layer optimization techniques.

The Open Systems Interconnection Model defines the various functions of a networking system. It enables the interoperability of various products and software. The model's seven main components are Physical, Data Link, Transport, Session, Presentation, and Applications. he Open System Architecture (OSI) was first introduced in 1984 by the international organization for Standardization. It is a conceptual model that describes how networks work as shown in Figure 1(a). The Open System Organization Model, first created in 1984, is a widely used framework for describing Network Architecture. The lowest layer of the OSI model is concerned with transmitting raw data bits across a network. It can be generally categorized as physical or optical data bits as shown in the Table 1. The data link layer provides a connection between the physical and logical nodes. It acts as a bridge between the physical and logical layers. The network layer is responsible for delivering frames from the data link layer to the destination. It uses logical addresses such as IP to route the messages. The network layer carries frames from the data link layer to the intended destinations. It uses logical addresses, such as IP, to get the destination. The presentation layer translates data that the application accepts based on the language or syntax that the application uses. It can also handle encryption and decryption. The end-user and the application layer are directly connected to the software application. The application layer manages all the details of the software operation.

Transmission power control based on MAC layer

The 802.11 wireless mediums are the original standard for Ad Hoc and infrastructure networks that use Distributed Coordination Function (DCF) in the MAC Layer function. In 802.11, the transfer data from source to destination done with the wireless mediums approach uses a bi-directional handshake procedure. The 802.11 wireless mediums use static transmitting control from source to destination to prevent hidden and exposed node problems. As a result, ad hoc networks increase energy consumption, conflict, and engagement. The ultra-high-layer design propagates the power control algorithm, which proposed to optimize the transmitted value. The idea of TCP in the MAC Layer is to utilize more exceptional communication capabilities for RTS (Request to send) and CTS (Clear to Send) packets as shown in Figure 1(b). The data-ACK packet provides the lowest power. In multi-channel MACs, there are two problems: (a) middle access and (b) co-channel interaction. Communication power control performs a vital role in solving issues. MAC layer directly affects the network layer to select the next hop. The dual-channel solution improves local reuse by using an extended power control system.



(a) (b)

Figure 1. (a) Typical OSI Wireless Reference Model. (b) The OSI Model, TCP/IP suite and MANET protocol stack

Table 1. Design parameters in cross-layer

Category of Network	Cross-Layer Issues							
	Mobility	Quality of Service	Safety	Power	Energy Supervision	Energy Consumption	Load	Position
Cellular Network	×	×	×	×	×	×	×	✓
MANET	✓	✓	×	✓	✓	×	×	×
Sensor Networks	×	×	×	×	×	✓	✓	×
WLAN	✓	✓	✓	×	×	×	×	×

3. PARALLEL WORKS

An extended power control algorithm, which reduces tension and increases the overall flow of the network. Interference and maturation of the databased optimization algorithm used to reduce conflict and energy consumption. Additional hardware such as transceivers needed to control transmission power. In a single channel with no additional hardware, a transmission power control uses the node's scattering power. The development of an algorithm that adjusts its transmission energy based on distance from the destination. In which the nodes determine their transmission power based on the distance from the source and the destination. At high transmission power, a method used to control the RTS sending power. Although it gradually increases RTS's power, CTS sends it to a higher transmission power to prevent data packets from sent to its neighbors. This process improves the throughput of network lifetime and decreases energy usage. It uses interference levels and uses RTS-CTS packets to energize neighbors and optimize their transmission power.

Excessive transmitting power increases link length and causes tension. In the event of a collision, the conflict window in the MAC layer increases. The algorithm is transferring energy to tuning, resulting in a controversial window. A similar method used to optimize the expansion power of the node. The topology of the network and the nodes' degree depend on the node's expansion power. If the node's transmit power is high, it has a high degree of correlation with the node's amplitude. Node degrees are essential for network performance.

Moreover, the power control system for power optimization, network connectivity, topology and optimal node degrees proposed. The cross-layer method to maximize local reuse, limit involvement and conflict. With high transmission power, RTS and CTS performed. In acknowledgments of data packets, the transmission control is equal to the power carrier range and interference range. With the RTE-CTS MAC, IEEE 802.11 reveals unseen node issues once the transmission control is less. Also, the node issue exposed when the transmission power is less. The unseen nodes in the network are available nodes to enhance three-dimensional recycling. High transmission power interferes with additional nodes, and then small transmission power causes link distortion. To address the relationship to contact and engagement between layers, the CLD considers parameters like delay, interference, and familiarity in MAC and physical layers. The link kernel operating system, power control to reduce interference between bandwidth capacity and increase bandwidth efficiency.

Network availability is essential on behalf of wireless nodes because wireless networks consume partial power sources. Power degrading attacks are serious issues from the node of the wireless network and reduce network longevity. Vampires attack Carousal and Stretch [9]. He proposed a plan to detect vampire attacks. In addition to creating simulations using NS2, they also used the algorithm to achieve this. They have tried to provide flexible solutions aimed at vampire power degrading attacks [10, 11].

Moreover, an investigative model is proposed [12] to approximate all node duration from the net lifetime setting. They analyzed power inclusive development and developed methods to enhance the time duration availability of net. Time duration technique All Node Died Time, First Node Died Time towards estimation in the remaining lifetime. The node energy prone to attacks leads to power holes. Power hole in words that describe the situation. Synchronous neighbors on the wireless network exchange packets for quick exits lead to malicious attacks with a stream of traffic. With the power hole, the lifetime of the network significantly reduced. Associated algorithms are Geographic Routing Algorithm and determined the emission time then power perforation order to minimize problems with energy holes.

Furthermore, Peng et al. [13] focusing on attacks on social networking sites. The anonymous attack is intensive in social networking sites. Even though it is private, information is still available to the public. It has the potential to be utilized by criminals to launch fraud attacks. The material is now out to the public, and anybody who comes across it will access it quickly. Even if the info in social sites keeps the amount of information disclosed to a minimum, the more personal the information becomes, the more susceptible it becomes. Social consumers provide more information, the greater the likelihood that they may be impersonated and deceived into allowing access to restricted websites and applications. Furthermore, Raikwar & Mishra [14], fraud attacks on wireless networks studied. They have made it difficult for counterfeit physical assets to detect fraudulent attacks, identify the number of attackers, and find obstacles. Energy computation discovered to determine supports by safeguarding the approach for the incidence of attacks. Marti et al. [15] designed the vampire attack simulation in wireless nets. A mechanism to optimize such attacks from the research is a typical vampire attack. These attacks not exact protocols and should not hinder the instant accessibility of networks. It uses messaging to follow protocol, low data transfer with high power consumption, no problem with detected routes. Therefore, it is challenging to detect vampire attacks. The vampire has proposed a method to reduce aggression. This process involves initiating the mitigation process, finding aggressive nodes. The blacklisting the vampire nodes discusses low-power wireless networks and power drain attacks on such networks. He highlighted the discovery and avoidance of such attacks by creating model evidence of thought.

On the other hand, Singh & Jain [16] were aware of the attacks, which ended batsmen's lives with modified packets. Instead of having to move unnecessarily before arriving at the destination, the packets arrive at the destination. This malicious activity can lead to the spread of energy over wireless networks to investigations conducted by Singh & Jain [16] performed geological investigations on carousel and vampire attacks. This work has prompted an additional investigation into power-drain attacks. It identified both attacks used legitimate but unnecessary packet durations to make energy and dust. Due to vampire attacks, the nodes look like real nodes and too small to resist them. Also proposed a method to identify and avoid similar attacks [17].

4. SECURE CROSS-LAYER DESIGN FOR AD HOC NETWORKS (SCLD-AHN)

The TCP/IP intended for wired access layers. Low bit error rate, fixed latency, reliability, dynamics and lack of transparency between layers in the link. The TCP / IP protocol suite consists of five layers, one layer acting on top of it. It can access services from the bottom layer through a transparent

layer. The SCLD-AHN protocol, by default, considers cross-layer parameters in other layer communication such as TCP/IP architecture provides precision and isolation of the components. Still, most conventions are compatible with wired networks. These are capable of resolving wireless linking, where the state of the channel depends on time and location.

Additionally, wireless links have less error rate potential, weak links, and user flexibility. The CLD design brings approximately unpredicted results. The common issue with TCP protocol in wireless network environments is the packet loss. The TCP estimates that cause congestion. Excessive sound link, blurring or interference between two channels or loss of equipment handoff. Besides, TCP / IP extensions in wireless networks cause many performance problems. Multimedia transmission through wireless linking, transmission power-sharing, security and power consumption are common problems. In the following sections, we describe the cross-layer security design issue.

4.1 CLD security design

Authentication and data are both important. Security elements like integrity, secure communication, and confidentiality are very important for a network to function properly and effectively. This article discusses several forms of attacks, dangers in MANETs, and a few examples of safe routing. The security parameter is required in cross-layer to ensure safe coordination between different layers to prevent multi-layered attacks. Multi-layer reduces unnecessary protection plans, reducing energy use and eliminating security delays is essential to airport security. Furthermore, in the TCP / IP model, the relation between layers is mutually independent. They employ their cryptographic transcription methods WEP, TKIP and WAP2 to use IEEE 802.11 standard IP protocol, TSL, and SSL protocols in network and transport layers, respectively. These protocols suffer from the bottleneck of high-performance issues and maximum energy utilization. These parameters play a vital role in coordinating other layers with the bottleneck in security protocols. If the data processing bottleneck exceeds its limits in the security protocol, the encryption in lower layers might affect the transmission, and then top layer security algorithms selected.

Usually, WSN is more prone to a variety of attacks. Stretch attack extends the length of packet paths, causing packets to be processed by a more significant number of nodes. Some packets of a route tranquil are introduced by carousel attackers in the form of a chain of loops, resulting in the same node appearing in the route several times. The suggested system tackles this difficulty by using approaches such as the Energy Weights Monitoring Algorithm and the Route Tracking Algorithm, which result in a significant reduction in energy usage. Once CLD aims to improve the QoS of video streaming over WSN, it is indispensable to safeguard it in the network. SCLD-AHN saves energy-drain attacks, such as carousel and dilution, removes power from the system and significantly reduces lifecycle, simplifying SCLD-AHN in the occurrence of attacks. The proposal provides procedures to protect SCLD-AHN from power-leak attacks. Layer design preserved using the proposed framework in this section. Thereby increasing security for SCLD-AHN.

The expansion of this technology has created many wireless system architectures, such as the MANETs, the VANETs, the Sensor Network and the Internet of Things (IoT) Cognitive Radio Networks. Additional security imposes massive computing overhead in the Media Access Control layer (MAC), transport and network layer. Wireless link optimization improves network performance. The basic idea behind cross-layer link optimization is more layers such as transport and applications adjust their parameters to accommodate differences in physical and mac layers. The drawback of existing layers boils down to solve in the present algorithm. However, they can degrade the performance of other parameters. Cross-layer communication between different layers is essential for solving these types of problems. However, optimization techniques still open challenges for future works.

The proposal specifies the CLD method for efficient secured video data broadcasting in WSN. Before proposing CLD, optimization assessed in the MAC and Physical layers. The basis behind this is that when a wireless network working with CLD becomes malicious, its performance deteriorates. Stretch and carousel attacks of power-drain attacks can overthrow SCLD-AHN's advantage by using power over wireless networks. This issue addressed by secure cross-layer design for ad hoc networks to protect against such attacks, Vampire Attack Prevention (VAP) algorithm implemented. VAP used with and without the apps. Observations made throughout the network's life, the remaining power of the network in routing load, delay, and the more active systems counter to various rounds.

4.2 Vampire attacks on wireless networks

Usually, stretch, carousel attacks referred to as vampire threats. Mutual threats lead to the spread of power over wireless networks. Such attacks are difficult to detect because they are legitimate, and messengers often appear to be real. When packets move through legitimate means to waste a node's energy before reaching the destination, they cause unnecessary energy transmission. In both attacks, a malicious root created using the original root defects.

4.3 Carousel attack

Opponents make violent attacks by building routes using indefinite iterations. The packets run under iterations loses its path needlessly. In circular iterations, the power of the packet drains, then it refers to a carousel attack. However, packets can legally move and detecting such attacks can be challenging. One reason for the attack was the lack of assessment in the title. The risk of wireless network and carousel attack shown in Figure 2.

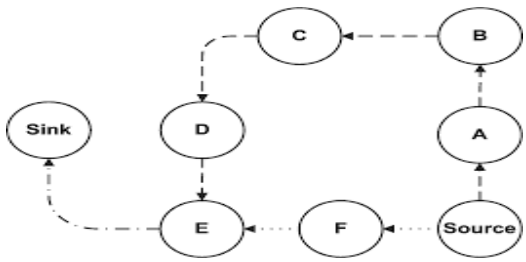


Figure 2. Carousal attack

As shown in Figure 2, wireless networks have A, B, C, D, E, and F source and destination networks. Figure two, with the arrow, shows the path of the carousel attack on the right. The

exact route from source to destination E. The packet loops before the carousel attacks reach the destination. The path to the destination to ensure that energy not wasted reached the destination without loops. Opponents inject malicious paths into packets. Therefore, attack-affected packets go straight to the traps without reaching the destination. After the injection loops completed, the packets arrive at the destination node.

4.4 Stretch attack

An attack based on basic routing errors. In this attack, the opponent creates more paths by adding additional nodes to a valid path. Instead of routing loops, the energy dissipates. It contains all the nodes in the network to join the sink node. Stretch attack surges the span of the path, and then it is determined to be a stretch attack. In this attack, packets unnecessarily moved to multiple nodes between the destination and the disaster, resulting in a power outage.

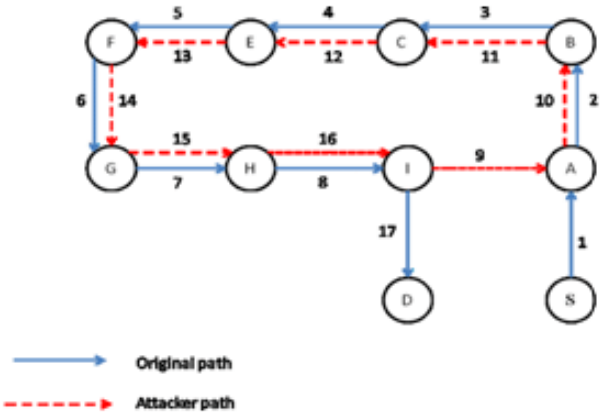


Figure 3. A typical stretch attack model

Figure 3 represents scattered arrows as an exact path amid the base and the sink. Instead, the substantial source (S) -> A ->B->C-> D-> E-> F-> G-> H->I->(D) destination indicates the destructive path from the end. The authentic way is from base ->A->I->sink. So, many unnecessary ways for dry power in nodes misused.

5. SCLD-AHN DESIGN AND ANALYSIS

There have been numerous attempts done in the past to define drain attacks that hold up the base station to attack. However, some studies extensively analyzed different routing protocols and named the carousel and stretch attack features of the two major power lap attacks. As mentioned earlier, these two attacks are the result of malicious routing on WSN. The data stream passes through malicious means created using an adversary through energy out of the network, resulting in the network lifetime decline. The effective method by Perno, Look, Gustad and Perig (PLGP) first developed to solve the packet-forwarding problem due to security flaws. PLGP modified the forwarding point of this method to be more lenient against fuel-exit attacks. The improved PLGP method found to be suitable for the protection of SCLD-AHNs explored in this section. The integrated optimization of a physical layer and MAC layers integrated into the SCLD-AHN protocol. This methodology designed to use and improve PLGP to enable SCLD-AHN for effective and secure multimedia broadcast over wireless networks.

A packet passes from one source node to sink, and data streams contain routing data, allowing it to move a specified route. However, in the presence of an attack, the packet is injected with the root's malicious structure. The use of PLGP in the proposed Vampire Attack Prevention (VAP) algorithm provides a secure means for data transmission. PLGP's topology search phase provides the correct information. The search result used in the next step is called a packet dispatch step. The topology detection stage states its summary and its other information. When using root search, it can help to find the right path. When attacked by malicious means, the method executing on individual node adds a symbol when a packet moves around. In other cases, any sign of iterations in the packet moves, the compromised node will find it. When packets forwarded to each node, potential vampire nodes checked to identify it, and then place required actions. The Vampire Prevention Algorithm (VPA) is as follows.

5.1 Vampire prevention algorithm implementation in SCLD-AHN

The VPA defends the SCLD-AHN system since power drain attacks. The reason for defense is to resolve CLD not to fail in QoS multimedia flooding. The proposed procedure increases the security of SCLD-AHN.

Algorithm 1: Vampire attack defense algorithm
Step i. Get started
Step ii. Packets sent from source to destination
Step iii. Attackers enabled over the network
Step iv. Fix packet transmission check
Step v. Vampire attacks have a backward propagation
Step vi. The 'PLGP' process has begun
Step vii. If (each node checks path history) Allow connections to non-neighboring malicious nodes
Step viii. Else, other packets checked, and it goes to the sink.
Step ix. If (Dynamic routing of node accessible) Validate and Update table << next node routing of Packets
Step x. Else If (Dynamic routing of a node not accessible) Validate and Update table << next-hop node routing of Packets
Step xi. Else Update table
Step xii. if (threat node's power ID) Update the routing table << destination ID
Step xiii. PLGP damaged by malicious search
Step xiv. Other packets that pass to neighboring nodes Then stop
Step xv. Else Normal transmission of packets
Step xvi. Sends packets to Sink
Step xvii. If concluded
Step xviii. End

When the algorithm runs on each node, any packets found in the looping or stretch path initiated by the opposition must reach the node and know its source. In addition, the history of the way the packet traveled. It effectively determines where the packet displays uncompromising behavior.

5.2 Simulation

This section provides targeted VAP results using wireless

networks for multimedia propagation and attack prevention on SCLD-AHN. Specific VAP evaluated using a variety of performance metrics. These comprise active nodes per round, the overhead due to complex routing, the source to destination, end delays, the number of rounds in-network, and the network's lifespan. These measures improve the QoS in multimedia broadcast contrary to power drain attacks on wireless environments. Experimental studies conducted using Omnet ++, where specific VAP results implemented without comparing SCLD-AHN to power-exit attacks.

5.2.1 Simulated settings

The metrics parameters such as end-to-end delay, nodes per round and the overhead in complex routing used to enhance security improvements in the VAP algorithm. The network lifetime calculated as Eq. (1).

$$\text{Network lifetime} = (I_t + S_t + P_t + R_t) * m \quad (1)$$

Here, I_t denotes the start time, S_t the sending time, P_t the stopping time, R_t the time point, m represents the total nodes. Remaining energy calculated using energy lifetime network in Eq. (2).

$$\text{Energy Residual} = \frac{I(E)(St + Pt + Rt)*k}{100} \quad (2)$$

Eq. (2) network lifetime variables and other parameters 'k' used as total rounds, also initial strength I (E) of the round. The rounds 100, 200, 300, 400, 500, 600,700, and 800 network lifetime, residual energy count and several rounds presented in Table 2. Establishment values are created by the simulated revalues. Prevention of power-drain attacks along with the target prevention algorithm. Similarly, the residual force energy attributed to Eq. (2) presented in Table 3. At the end of the computational delay, according to Eq. (3).

$$\text{End-to-end Delay} = \text{Total Node Delay/Number of Nodes} \quad (3)$$

If the total number of packets counted, the count for each packet delayed. Therefore, the following illustrations describe the end of delay calculations.

Sample calculation

j= Id (Sequence number) of the packet.
Delay[j]= Time Delivered [j] – Time Dispatched[j]
Total Delay[j]= Delay[j] + Early Delay [j]
Average Delay[j] = Total Delay[j] / Count
Delay[j] = |9.2-16.8 | =7.6
Total Delay[j] = 0+7.6
Average Delay[j]= 7.6 / 1.2 = 6.3

The routing overhead is taken as a quantity parameter in the assessment process to find the number of routes the packets pass.

5.2.2 Simulation results and discussion

Wireless networks analyzed to provide CLD flexibility against carousel and stretch attack to provide a better quality of multimedia streaming using SCLD-AHN. Omnet++ used to evaluate the security parameters in the CLD design. The parameters intended to evaluate and prevent power-exit attacks using the VAP algorithm. The parameters include end-to-end delay, nodes per round and the overhead due to routing to measure performance metrics. The Table-2 results show the lifetime of nodes with and without VAP technique. As noted above, resistance compared to attacks with and without attack.

Table 2. Lifetime of network in different rounds

Nodes Considered	Life Time of Network with different Rounds	
	Without Prevention Algorithm	With Prevention Algorithm
100	1050	3300
200	1035	3150
300	900	2850
400	1200	3000
500	1275	3000
600	900	3150
700	900	3450
800	1350	3600

Table 3. Number of attack sequences with and without network energy

Number of Rounds	Residual Network Energy (%)	
	Without Prevention	With Prevention
20	120	90
40	120	90
60	120	90
80	117	93
100	119	68
120	113	68
140	113	60
160	113	59

To monitor multimedia broadcasting performance with and without VAP algorithm. The network lifetime affects the number of nodes as per the experimental facts. As the number of nodes increases, the network lifetime increases when attacks block the VAP algorithm, the network lifetime increases.

Preventing an attack In Figure 4 horizontal axis, the vertical axis represents the total number of nodes and the number of rounds the iterations conducted in the simulator. The total node considered are 100, 200, 300, 400, 500, 600, 700 and 800. It observed that if nodes increase, then lifetime affected. Similarly, network lifetime increases if attacks disallowed using the proposed technique.

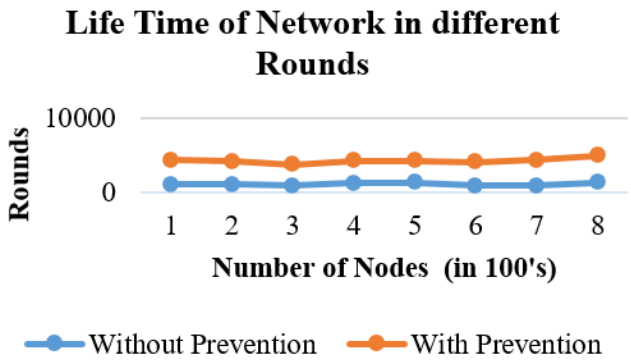


Figure 4. Lifetime of network with the number of nodes and rounds

Table 4 shows the total capacity of the network and total nodes. It observed that if the attacks are stationary, then the rest of the power improved. The total rounds in-network affects the power remaining with the network.

Resistance In Figure 4 horizontal axis, the vertical axis represents the total rounds and energy remaining throughout the network with a certain number of rounds. Number of rounds are 20, 40, 60, 80, 100, 120, 140, 160. Increasing the number of rounds affects the remaining power of the network as shown in Figure 5. When attacks stopped using the proposed algorithm, the force remaining in each observation round is greater.

Table 4 displays the experimental results corresponding to the number of nodes, with prevention and without prevention of attack resistance mechanisms. The observations indicate that the delay from end to end affects total rounds in the network. If rounds increased, then the delay is increased.

Table 4. Number of nodes for delayed and non-delayed attacks

Nodes Considered	Delay End to End (in ms)	
	Without Prevention Algorithm	With Prevention Algorithm
100	30	3
200	33	5
300	35	6
400	36	8
500	38	9
600	39	11
700	41	12
800	42	14

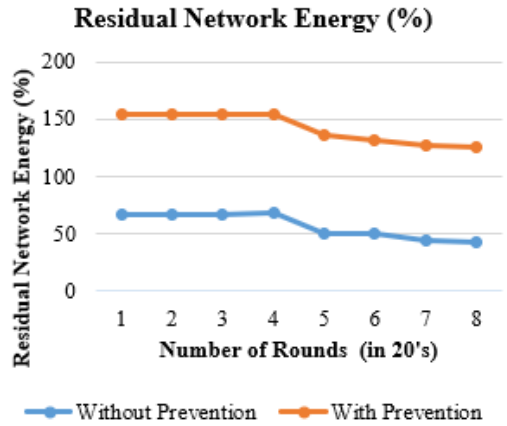


Figure 5. Limit the number of forces in the presence and absence of attacks

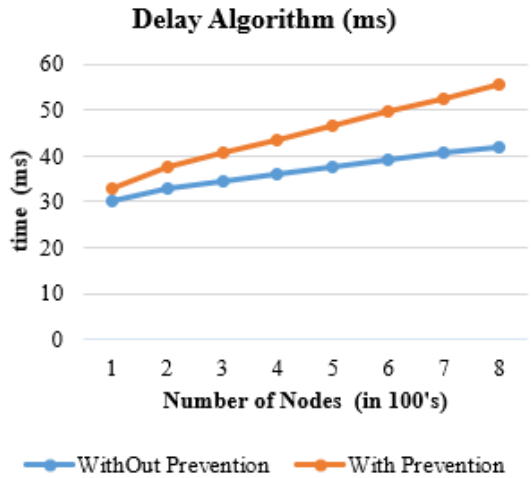


Figure 6. The number of nodes with and without attack resistance

Table 5. Number of overhead routing nodes without prevention and prevention

Nodes Considered	Comparison of Overhead in Routing	
	Without Prevention algorithm	With Prevention algorithm
100	20000	10000
200	30000	12000
300	38000	14000
400	38000	18000
500	42000	19000
600	56000	20000
700	56000	21000
800	60000	22000

The Figure 6 represents nodes used in the experiment are 100, 200, 300, 400, 500, 600, 700 and 800. The horizontal, vertical axis represents total nodes and final delays, respectively. By preventing attacks, the delayed end significantly reduced.

The results of total nodes and overhead in routing represented in Table 5. The observations show that total nodes in the network affect the overhead path. Overhead reduction occurs if attacks prevented using the proposed algorithm.

As shown in Figure 7, the horizontal, vertical axis represents total nodes and routing overhead correspondingly. The total nodes simulated are100, 200, 300, 400, 500, 600, 700 and 800. It observed that if routing overhead increases as the number of nodes increased. However, these attacks were blocked by the VAP algorithm, then routing overhead reduced compared to the non-blocking of algorithms.

Table 6 shows rounds and live nodes in with several rounds in the network. If rounds increased in the network, then real-time nodes increased.

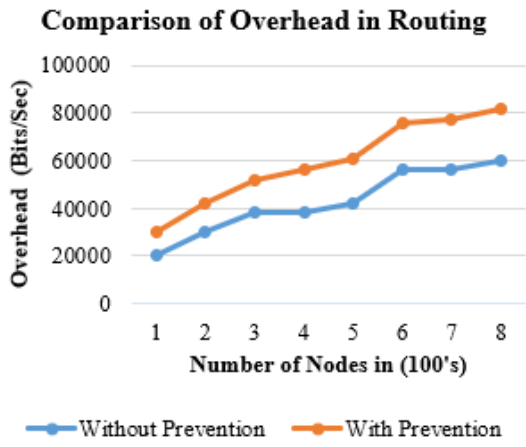


Figure 7. Node count vs. routing overhead and lack of attack block

Table 6. The nodes with and without attack resistance

Nodes Considered	Nodes in Traffic State	
	Without Prevention Algorithm	With Prevention Algorithm
500	800	800
600	800	800
1000	620	800
1500	640	800
2000	560	720
2500	480	640
3000	400	720

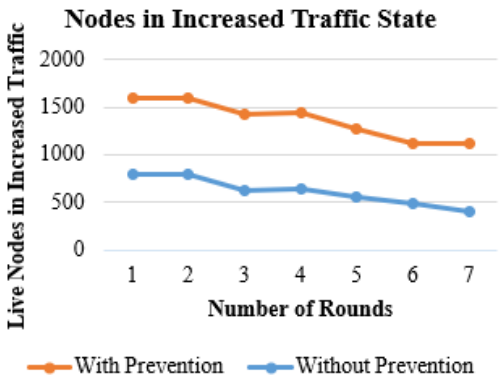


Figure 8. Number of live nodes and attendance range

Lack of offensive protection As shown in Figure 6, horizontal, vertical axis depicts total rounds and live nodes, respectively. The live nodes with 500, 600, 1000, 1500, 2000, 2500 and 3000 different rounds as shown in Figure 8. It observed that if live nodes decline, then total rounds increased. If the power-drain attack was blocked, the number of active nodes against the various numbers increased significantly.

5.3 Discussion

The proposed CLD design embedded between the MAC and physical layers. The physical layer maintains the energy control using QoS with higher-level layers. Simulation experiments have shown that physically improves the QoS of multimedia data transfer in wireless channels. The QoS parameters end-to-end delay, throughput, and delivery ratio by 40%, 30%, and 60% of average reduced ratios. The MAC layer optimized to test performance gains. Preferences used for data packets in the MAC layer. The precedence obtained by the length of the sag and hop. The possibility of expansion with the MAC layer also considered. It is not a time interval, but the node has the right to start the transmission.

The results summary of average end-to-end delay by 70%, while the energy efficiency increased by 18%. The packet delivery throughput ratio enhanced by 18% and 75%, respectively. Results in the underlying mac layer found to classify media coverage in wireless networks. The results show an average end-to-end delay of 25%, average packet delivery ratio of 45%, average throughput of 29% and average efficiency of 15%. Another cross-layer design developed to investigate further the limitations of MAC and physical layers.

In contrast, energy variation and power are significant parameters in the physical layer. An integrated CLD method combines two layers with other layers for more comprehensive optimization. It estimated against packet error rates in the case of PSNR and PSNR using the Evolution Toolkit. Optimization combined with the proposed CLD improved performance compared to other CLD methods. Simple masking with interest-based error masking in the literature. QS Is 8% dB higher than the average PSNR and 1% dB higher than the most straightforward ROI technique? Multimedia transmission with SCLD-AHN showed a 60% improvement in PSNR without using SCLD-AHN. Security improvements made to SCLD-AHN to protect against forced-exit attacks such as carousel and stretching. Therefore, SCLD-AHN performs its essential features to enhance secured video broadcasting over wireless channels through the proposed Vampire Attack Prevention (VAP) algorithm. The algorithm uses the SCLD-AHN running network, which protects the network from malicious attacks, protecting it from power destruction and vulnerability. With increased security, SCLD-AHN showed a 76% increase in average lifetime and a 36% increase in average remaining network power. The average end-to-end delay against the different active nodes is 76%. The average routing overhead is 72%, and the average number is 20%.

6. CONCLUSION

The purpose of the secure cross-layer design (SCLD) is to embed the VAP algorithm to prevent stretch and carousel attacks in wireless networks. These types of attacks belong to energy-drain, which leads to damage the multimedia transmission in various wireless network applications. It utilizes routing algorithms to interrupt power. Stretch, and carousel attacks use the potential to affect the way the packets move to reach the end. The carousel causes an attack before the packet arrives at the destination.

Meanwhile, the stretch attack is expanding to include unnecessarily new valid nodes after a stretch attack. Therefore, both attacks carry packets in a hostile manner before reaching the destination. SCLD-AHN provides enhanced multimedia transmission over a wireless channel network to steps for the SCAP-AHN system to protect against malicious power-exit attacks. SCLD-AHN is subject to security enhancement. Experiments carried out to prevent carousel and stretch attacks. Omnet ++ simulations performed to prove the proof of idea. The results depict the VAP algorithm in wireless networks prevents power drain attacks. It validates SCLD-AHN's ability to provide better-secured multimedia transmissions in wireless networks.

REFERENCES

[1] Thylashri, S., Femi, D., Manikandan, N.K. (2018). Efficient mechanism for recognize and avert vampire attacks in wireless sensor network using Parno, Luk, Gausted and Perrig method. Journal of Computational and Theoretical Nanoscience, 15(11-12): 3486-3491. https://doi.org/10.1166/jctn.2018.7650

[2] Perkins, C.E., Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review, 24(4): 234-244. https://doi.org/10.1145/190314.190336

[3] Kurode, E., Vora, N., Patil, S., Attar, V. (2021). MANET routing protocols with emphasis on zone routing protocol–an overview. In 2021 IEEE Region 10 Symposium (TENSYMP), pp. 1-6. https://doi.org/10.1109/TENSYMP52854.2021.9550879

[4] Soumya, S., Bappalige, N.N. (2021). Performance analysis of mobile ad hoc routing protocols in vehicular ad hoc networks using NS3. International Journal of Applied Engineering and Management Letters (IJAEML), 5(1): 19-28. https://doi.org/10.47992/IJMTS.2581.6012.0124

[5] Ghildiyal, S., Mishra, A.K., Gupta, A., Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. IJRET: International Journal of Research in Engineering and Technology, 3: 2319-1163. https://doi.org/10.15623/ijret.2014.0322030

[6] Vafaei, M., Khademzadeh, A., Pourmina, M.A. (2021).

A new QoS adaptive multi-path routing for video streaming in urban VANETs integrating ant colony optimization algorithm and fuzzy logic. Wireless Personal Communications, 1-34. https://doi.org/10.1007/s11277-021-08142-7

[7] Estrin, D., Girod, L., Pottie, G., Srivastava, M. (2001). Instrumenting the world with wireless sensor networks. In 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221), 4: 2033-2036. https://doi.org/10.1109/ICASSP.2001.940390

[8] De Cicco, L., Mascolo, S. (2013). An adaptive video streaming control system: Modeling, validation, and performance evaluation. IEEE/ACM Transactions on Networking, 22(2): 526-539. https://doi.org/10.1109/TNET.2013.2253797

[9] Verma, D., Singh, G., Patidar, K. (2015). Detection of vampire attack in wireless sensor networks. International Journal of Computer Science and Information Technologies, 6(4): 3313-3317. https://doi.org/10.1.1.695.2554

[10] Vasserman, E.Y., Hopper, N. (2011). Vampire attacks: Draining life from wireless ad hoc sensor networks. IEEE Transactions on Mobile Computing, 12(2): 318-332. https://doi.org/10.1109/TMC.2011.274

[11] Ren, J., Zhang, Y., Zhang, K., Liu, A., Chen, J., Shen, X.S. (2015). Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks. IEEE Transactions on Industrial Informatics, 12(2): 788-800. https://doi.org/10.1109/TII.2015.2411231

[12] Juneja, V., Gupta, D.V. (2018). Security against vampire attack in ADHOC wireless sensor network: detection and prevention techniques. In International Conference on Wireless Intelligent and Distributed Environment for Communication, pp. 25-38. https://doi.org/10.1007/978-3-319-75626-4_3

[13] Peng, W., Li, F., Zou, X., Wu, J. (2012). A two-stage deanonymization attack against anonymized social networks. IEEE Transactions on Computers, 63(2): 290-303. https://doi.org/10.1109/TC.2012.202

[14] Raikwar, M., Mishra, P. (2017). A mitigation approach to protect wireless sensor networks over vampire attack. International Journal of Computer Applications, 159(7): 25-28. https://doi.org/10.5120/ijca2017912994

[15] Marti, S., Giuli, T.J., Lai, K., Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 255-265. https://doi.org/10.1145/345910.345955

[16] Singh, S., Jain, P. (2017). Detection and prevention for avoidance of energy draining vampire attack in MANET. Int. J. Adv. Res. Comput. Sci. Softw. Eng, 7(5): 966-970. https://doi.org/10.23956/ijarcsse/SV7I5/0200

[17] Vasserman, E.Y., Hopper, N. (2013). Vampire attacks: Draining life from wireless ad hoc sensor networks. International Journal of Research in Computer and Communication Technology, 4(8): 586-593. https://doi.org/10.1109/TMC.2011.274