A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks

Keshav Kumar 1, Sahil Verma 1, Kavita 1*, NZ Jhanjhi 2, M N Talib 3
1 School of Computer Science and Engineering, Lovely Professional University, Phagwara, India
2 School of Computer Science and Engineering, SCE, Taylor’s University, Malaysia
3 Papua New Guinea University of Technology, Lae, PNG, Papua New Guinea

Corresponding author: kavita@ieee.org

Abstract—In this paper, we are going to evaluate various wireless network security related issues and how do they affect the quality of service of a wireless network and Mobile AdHoc Networks(MANETs). The time systems are increasingly required Getting educated more and more. Systems are simple Drastically converting the structure into more functional and dynamic. Computer networks have undergone a major move from cable to wireless A recent development has been networks and fast wireless infrastructure. MANET has appeared between many other cellular networks. Why? Why? dynamic topology without any centralization, conventional path MANETs do not comply with protocols and authentication systems. These MANETs are responsive to a lot of people It is not feasible in other networks to attack and participate in disruptive operations. A Wireless Network can be a very vulnerable entity and is always susceptible to various types of attacks and attackers, we are going to discuss a few of these attack and how do they affect the overall network performance, finally we are going to evaluate some of the solutions offered and how they improve the network.

Index Terms—Network, Architecture, Network Security, Wireless Networks, Application Security, Mobile AdHoc Networks, MANETs, Sensor Nodes.

I. INTRODUCTION

A wireless network is a computer network not connected by any type of wireless medium. However, On the other hand, a MANET is a set of wireless sensor nodes that are linked together through a base station. Wireless nodes are a group of MANETs. Nodes are feasible Easily enter and leave the network when it is not available Intermediate support. Inter-mediate support. Because of these routing issues, There are several types of attacks in protocols that are not protected A big intrusion is wormhole intrusion on the network layer. We use MANET to find and prevent these attacks Aspects of defense [16]. We will address them in this article Using multiple approaches.

First of all, this text gives an Architecture of MANET of nodes classified Two forms, namely mobile trusted nodes and mobile trust Nodes. Nodes. The mobile nodes of faith and confidence look like Specialized and non-specialized respondents the site of the tragedy. Trusted mobile node affiliation with In its correspondence, one of the trusted moving nodes Range indicates the accident site’s land situation. The use of a wireless network makes it possible for businesses to prevent the expensive process of cable deployment in buildings or as a bridge between various installation locations [1]. The following are 4 different types of cable network links, which keep the world connected: wireless systems based on radio waves that are physically introduced at network architecture level:

1. Wireless Local Area Network(WLAN): Links two or several devices using a mobile distribution
method to link to the broader internet via access points.

2. **Wireless Metropolitan Area Networks (MAN):** In a wireless MAN, two or more (W)LANs are linked to each other.

3. **Wireless Wide Area Network (WAN):** A Wide Area Network links large areas or cities.

4. **Wireless Personal Area Network (PAN):** A Wireless Personal Area Network links devices that are close together, that is within the reach of a person.

A wide variety of network with various usability and functionality helps bring us an era of wireless communication. Wireless communication is now a trend and everything is now becoming wireless, this is raising many concerns that the pre-existing network might not be capable of handling them now or maybe in the coming years, someday it is going to break and if it will the effects will be devastating and will impact billions of lives. A mobility model correctly representing the mobile nodes (MNs) that will ultimately use the protocol in question is important if the current protocol for an ad hoc network is to be simulated extensively. It is only in such a situation that the protocol proposed will be decided how it is applied. The Ease of use that the wireless networks and wireless network devices provide also comes with a completely new set of issues that were non-existent before the wireless communication networks took over, following are the issues that came into the picture:

- Connectivity Issues
- Security Issues
- Network Expansion Issues
- Access Point Issues

Security issues in a wireless network can be a lot more challenging and even more important to deal with as unlike a wired network unauthorized access can be done off-site without any physical connection and it complicates things a lot.

II. DIFFICULTIES IN COMMUNICATION AND TRANSMISSION WITH WIRELESS AND AD-HOC NETWORKS

Wireless sensor networks are a mobile computing area that emerges. In the ad-hoc environment, there are various challenges. This is partly attributed to their lack of money. They are normally installed in emergencies, for temporary activities or simply when no resources are available to establish complex networks. Consequently, in all networking sectors, ad-hoc networks generate new conditions and challenges. Conventional network technologies are necessarily not enough to deliver effective ad hoc operations. There are many security issues because of the wireless nature of contact and the absence of any security infrastructure. We try to analyse the requirements of the ad-hoc environment in this paper. We concentrate on ad hoc routing. The biggest problems in these fields have been dealt with here[22]. These questions, which have been active areas of study, we have sought to address.

Since communication will be through the wireless medium, communications can easily be reached by any intruders. Wireless networks have inadequate security and control signals associated with routing can be changed. The wireless medium may interfere with, interfere with, squeeze out, or distort. An attacker can quickly split up to understand or disrupt confidential routing[22] information, avoid routing information from spreading or even disrupt signals, and exploit routes by distorting them. To manage such matters, protocols for routing should be well adopted.
Major factors that come into play to restrict the capabilities of various wireless technologies:

- **Harsh Outdoor Environmental Conditions**: The topology and wireless network communication in electricity systems environments will change due to failures of the connection. Besides, RF interference, highly-caustic or corrosive environments can also be subject to sensors. Moisture, vibrations, soil and emissions or other performance-challenging situations. These harsh portions of sensor nodes can cause faulty environmental conditions and dynamic network topologies. Or rendering it obsolete to collect information.

- **Reliability**: A broad range of implementations for smart grid WSNs will have various standards and criteria for quality of operation in terms of stability, latency, network performance, etc. Moreover, as data collected is normally time-sensitive, such as electricity systems incidents, it is often necessary to obtain requirements systematically at the base station.

- **Resource Constraints**: WSNs are limited to three resources: a) power, b) memory and c) processing for development and implementation. In basic, the battery energy supply of sensor nodes is reduced. That’s why WSN contact protocols are largely designed to deliver high-intensity performance.

### III. WIRELESS NETWORK ARCHITECTURE

The standardising community for mobile ad testing in 1996 The Internet Engineering Task is used for ad-hoc networking The MANET workgroup (IETF) has been set up by Coercion. By the way, aim to standardise the features of the IP routing protocol for applications for cellular routing. A communication network infrastructure that provides the network connectivity, communications, operations, and maintenance of a company network for equipment, facilities, and software components across the network[2]. In most business IT environments wireless infrastructure is generally part of the IT infrastructure. The whole communications infrastructure is interconnected and used in real-time for data and information processing or access. Machine architecture is a way to describe everybody basic elements of a structure, such as groups, objects, Architecture, each part has interfaces and System data interaction must be a system convince an industrial or accurate requirement and necessity In the process of engineering, social contact.

Infrastructure refers to the computing resources which make possible network or internet connectivity, management, business and communication. Usually, the network infrastructure consists of both hardware and software and allows user-to-service, device and process computing and communication[3]. The network and IT systems are equivalent. They can mention the same thing at times, the differences between the two may also be subtle. The broader and more inclusive concept is often seen as an IT infrastructure. IT architecture (or IT infrastructure) describes a set of IT elements that are the basis for IT services. IT
infrastructure The IT architecture often refers to physical components such as hardware, but may also include network components or software.

**IV. COMPARATIVE STUDY**
In this section, we look at a few of the authors that are referenced in this study in brief about their various views and approaches regarding tackling various network related attacks.

Table 1. Comparative study of different referenced research materials

| S. No. | Reference | Issue                                      | Actions                                                                 |
|--------|-----------|--------------------------------------------|------------------------------------------------------------------------|
| 1      | [4]       | Wireless network security issue            | The author(s) have studied various networks and the preventive measures deployed in them. |
| 2      | [13]      | Next-gen network model security issues     | The author(s) talk about new security models that can be implemented that could help counter some major security issues in current times. |
| 3      | [10]      | Hello Flood attack                         | Authors did extensive study on hello flood attacks in a network and proposed a framework to help counter it. |
| 4      | [14]      | Risk Factors involved in using a wireless network | The authors stated no matter who is using the network certain amount of risk is always involved and how modern security standards can help reduce. |
| 5      | [8]       | Attacks on Wireless Sensor Networks        | Main deal of this research was to analyse different types of attacks on a sensor network and how do they effect the network and finally some standards to help prevent a lot of damage. |

V. SECURITY IN WIRELESS AND WIRELESS SENSOR NETWORKS

Assignment of sensor networks Reduced problems, hence conventional safety systems and are not used by conventional networks by today’s wireless networks. The network of the sensor. Inadequate control, loading and loading of sensor units capacity to connect. When the WSNs seem to be in an adverse setting, defence,
since they have different forms of violence, is quite essential. An assailant, for instance, You can easily eavesdrop, duplicate node data or intentionally provide traffic Disappointing sensor node info. The network of wireless sensors closely related to Current protection concerns impacting their physical environments. The sensor as results In an unknown free, unsupervised environment, nodes are mounted,

- Processes are not enough and fresh thoughts are required. WSN has a wide size. The overall number of nodes within the defence implementation network.
- An opponent will only inject malicious nodes into the network of sensors.
- The network of wireless sensors uses wireless communication between nodes, It’s mostly easy to eavesdrop on.
- For such network nodes, the source restriction is necessary Protection Protection. Store, control, submit packets of data.
- The considerations are high and too rough.
- The symmetric method of cryptography is being used as a substitution.

Performance, honesty, standard safety goals for wireless sensor networks Privacy, affordability, authentication, survivability, freshness and scalability. The network of wireless sensors is vulnerable to many attacks Unattended use in unregulated settings. To ensure safety Equipment. In WSN are multiple cryptographic methods such as symmetry and asymmetry Suggested. It is necessary to be able to authenticate to achieve protection in WSNs Transform data between sensor nodes as well as encryption.

VI. ISSUES IN THE SECURITY OF WIRELESS NETWORKS AND WIRELESS SENSOR NETWORKS

The risk of WLAN attacks on wireless networks is increasing as wireless LANs are deployed in almost any type of setting. There are several different reasons, but this is mostly due to a lack of knowledge about the wireless network[1]. Unlike a cable network, a physical connection to a computer is needed for a wireless system. This article examines some fundamental principles of wireless security and looks at some of the most common hazards in wireless networking[4]. There are quite several basic principles to be recognized by a person or business when a wireless network is deployed. This is very crucial when using a wireless network because the level of interference that is exposed to depending on the particular environment influences the network[2][4]. The first one is the basic understanding of which frequency is used by the system being used. Two major frequency channels (802.11), including the 2.4 GHz and the 5 GHz bands, are commonly used for wireless connectivity. From the point of view of defence, frequency selection has no significant impact on network security risks. What is affected is the amount of non-overlapping available channels in the network; most of them don’t affect protection unless an intruder attempts to interrupt or block a particular frequency to compel wireless terminals to switch access points[5].

Endpoint devices identify Wireless modems via SSID with security parameters. SSID identifies wifi networks. The SSID is transmitted from APs for most wireless networks, which allow customers to easily integrate. The SSID can not be transmitted with little technical bits of knowledge, which provides a little protection from wireless network attackers; however, this is not a very successful safeguard for a professional wireless intruder.
VII. TYPES OF ATTACKS ON WIRELESS NETWORKS

The safety and security of wireless communication require all steps to prevent unauthorized access to or harm to the information transmitted through wireless networks. The fact that airwaves appear to snoop somebody with an RF antenna has undermined most of the current protection architectures[14].

The wireless technology in our new networks is moving ever forward. Wireless links have one significant drawback health – as easy as they are. Securing communications technology poses a further challenge in comparison to their wired counterparts[5]. Different methods will allow wireless attacks against you. You should talk about WiFi mainly. Some are tricky, others are using brute force, and some people are looking for people who are not troubled to protect their network.

Many of these assaults in the real world are interconnected. Here are some of the types of attacks you might experience:

A. Sinkhole Attack:

Wireless Networks are sensitive to a widespread number of attacks, one being the sinkhole attack[14]. This attack is the best possible route to the base station that a malicious node advertises itself to confuse its neighbours further. The malicious node has the chance to manipulate the data, damage the regular use or even face many additional network security obstacles[7][6]. It’s a targeted assault on transmission. The node leaks into the network, which pulls all data packets on itself, functions as a sink node. Each network traffic is at risk in this attack[8]. By allowing the selective forwarding attack, Sinkhole attack will alter the packet flow direction. It attracts especially his neighbouring nodes to a dangerous node. The environment needed to attack Wormhole can be provided. That, by telling the neighbour clusters it is a sink node, suppresses messages in a particular region[8], While allowing the selective forwarding attack, Sinkhole attack will alter the packet flow direction. It attracts especially his neighbouring nodes to a dangerous node. The environment needed to attack Wormhole can be provided. That, by telling the neighbour clusters it is a sink node, suppresses messages in a particular region[8].
Fig. 2: A Sinkhole attack in progress

B. Selective Forwarding Attack:

Malicious nodes refuse the request to facilitate such packages to ensure that certain packets are not further exchanged through this form of network attack. The opponent may selectively or arbitrarily drop packets. In response to the packet error rate, the attacker attempts to change the Network. Furthermore, Selective forwarding is of two types:

- **Insider Attack**: Confirmation of the approved sensor nodes may be corrupted, or even the opponents may certain nodes and attack the entire network from any key or data. Such an incident is difficult to identify.
- **Outsider Attack**: The route among both genuine nodes is blocked and the path between genuine nodes is jammed.

Malicious nodes in a selective transmission attack It’s a black hole and can hesitate to move any. Only lose messages to make sure they don’t Any more propagated. Yet such a fighter is moving the threats of the nearby nodes that she failed And plan to search for a new path. A subtler sort of The assault is where the opponent moves packets systematically. A competitor who tries to uninstall or change packages Originating from a variety of chosen nodes, the Traffic persists and suspicions for their misdemeanour are restricted.
C. Sybil Attack:
A node is a multi-identified assault. Therefore an opponent can be in different places at the same time. The attack on Sybil significantly reduces the performance of fault-tolerant systems[8]. Sybil Attack is a form of attack that occurs in peer to peer networks where a network node actively works on multiple identities while undermining reputation system oversight/strength. The purpose of the attack is to manipulate the network in large measure in order to carry out illegal operations in the system (with respect to network rules and laws). The ability to build and operate false identities (user accounts, IP address records) is inherent in a singular entity. These hundreds of fake identities seem to be true, unique identities for outside observers[8][9].

The Sybil attack is also known as the 51 Percent attack, which implies that the attacker will try to own more than 51 per cent of the total traffic in the network and by doing that, the attacker can gain full control of the network and can even dismiss any previous authority or restriction already present in the network. Intruders might vote out of honest network nodes if they create sufficient false names (or Sybil identities). You will then fail to provide adequate reception or transfer blocks and restrict other network users effectively. Over the years, computer scientists have spent a long time studying how Sybil attacks of differing amounts of efficacy can be identified and avoided. No assured protection exists right now.
There are two types of Sybil Attack[9]:

- **Direct**: True nodes are directly attacked by the Sybil nodes.
- **Indirect**: Good nodes are attacked through infected Sybil nodes by establishing a link between the god node and the malicious Sybil node.

In order to signify an attack in the sense of peer-to-peer distributed networks, Sybil Node was the word “assault Sybil” first introduced in the language. Sybil attempts in wireless sensor networks in which the contact channel is available and distributed are especially quick to initiate. A Sybil node can monitor voting on group-based decisions by broadcasting messages with multiple identifications and even disturb network services compared seriously. Both spoofing and SYBIL can have a big effect on network efficiency through identity attacks. Cryptographic authentication is used for traditional approaches to preventing attacks by identity.

![Fig. 4: A Sybil attack in progress](image)

**D. Wormhole Attack:**

The attack in Wormhole is a serious attack in which two attackers strategically locate themselves in the network. The attackers will then continuously listen to the network and record the wireless data[11]. An assailant who cracks into a part of the system receives messages via a low bandwidth connection and also can repeat them through a tunnel in various sections. An opponent might persuade nodes that usually come from the simple station to be multiple hops that they are just a hop or two from the vermillion. This might create a falling hollow: if an enemy would artificially have a high-quality path to the base station on the other side of the wormhole, theoretically all the traffic around it is drawn if alternating roads are much
smaller.
Using a private path, which is called a tube, a wormhole attack uses two or more malicious nodes. The goal is for the rescue workers at the disaster scene to connect trustworthily and securely. Given the problems found in the subproblems, the following can be described[16].

When a wormhole exploit is made, at some point in the network, the attacker receives packets and then tunnels them to another part of the network and plays them back in the network. In a wormhole assault, two compatible tunnel nodes and data packets are intertwined with each other, in order to create a shortcut to the wireless network. Such a minimal-latency tunnel between both the two nodes will presumably increase the likelihood that it is chosen as an active path.

In the event of reactive protocols such as DSR and AODV, this attack could start directly by tunnelling each REQUEST to the objective node. If the adjacent nodes in the country of destination receive this REQUEST packet, they must retransmit the REQUEST packet and discard any other REQUESTs on the very same path for the process of discovery. This, therefore, prevents the discovery of roads other than the wormhole. This helps the attacker to launch an assault on the infrastructure as it controls virtually all routes found after a wormhole[11]. The WSNs are being seriously threatened by Wormhole Attack. Wormhole assault in WSNs has been one of the major attacks whereby a malicious node packs packets from one location in the network to a distant point in time[12]. Therefore, in a wormhole assault, since assailants are linked directly towards the other nodes in the WSN, they can communicate at a fast speed.

![Fig. 5: A Wormhole attack in progress](image)

**E. Hello Flood Attack:**

Some protocols for routing wireless sensor networks allow nodes to send hi signals to their neighbour. A node that gets a message should conclude that the communication should be within the radio range of the transmitter. This theory may be incorrect in some situations, though; sometimes an on-the-job attacker or other information with ample transmission power may persuade any other network node that the attacker is his neighbour. The intruder persuades a node to be a friend. False information with high transmitting
capacity can be transmitted. Many of our neighbouring nodes allow HELLO packets for broadcasting. The HELLO node presumes that the transmitter is in the signal range. The HELLO flood attack aims at slowing down transmission through network confusion.

The nodes or broadcast is taken in this attack advisory HELLO messages and announce your neighbour to yourself. If so, This message is given to a node and assumes that the sending Connection node is at the beginning of the node to communicate with and join the node As a friend, routing table. In a network, for example, The base station interacts with all sensor nodes By the neighbour’s way. When an intruder in a laptop class Captures or generates a legal node, Transmit a message to all the nodes in order to maximise the strength Massage induces doubt about the coming message To the nodes of her neighbour. Both nodes then take on board The Hello message path from the simple station is the shortest, assuming that the attacker node is a foundation. The station and the intruder interact. That’s what it feels like. Network and base attacker can easily monitor The resort and are cut from the network altogether.

The key attack in the network layer is the Hello flood attack. Hello, flood attempts may be triggered by a node that transmits a high power hello packet, such that a huge number of nodes in the network select it as the parent node even at a distance. Both messages must be forwarded to this parental multi-hop, that raises the lag. Hello, packets are sent in a wide region of the network to a large number of nodes.

![Network Diagram](image_url)

**Fig. 6(a):** Victim network before any attacker establishes it self
**F. Spoofed Attack:**

A spoofing attack is where a malicious party puts other user or computer on infrastructure in order for network hosts to be targeted, data compromised, malware distributed or access controls to be bypassed. There seem to be various ways of malicious assault that can be used by threat actors. Perhaps one of the most popular strategies is spoofing of the IP address, spoofing of ARP attacks and spoofing of servers. Often TCP/IP Suite protocols have no security measures for both the source or destination of the packet, rendering them susceptible to spoofing attacks if adequate steps are not taken for implementations to ensure that the transmitting or receiving host is similar. In specific, IP spoofing and ARP impersonation attack can be used to exploit a middle assault on hosts in a network of computers. The use of firewalls that deeper packet inspections or the use of measures to verify the sender or receiver of a message can mitigate spoofing attacks which are using TCP/IP suite protocols. Spoofing is the way to disguise of message or identification with which a trustworthy authorised source is associated. Spoofing threats can take many forms, from the known threats on phishing to caller ID spoofing used frequently to cheat the system in email spoofing. More technological aspects of the network of an entity could be attacked as well as a spoofing attack, such as IP address, domain name system (DNS) or ARP service.

**Fig. 6(b):** Victim network after an attacker sends falsified hello messages to establish itself as a neighbour and route packets towards itself
VIII. DELIBERATION FOR SECURITY IN WIRELESS NETWORKS

Security evaluation is based on network security objectives. The different dimensions of safety can reflect these security aims. Seven of these are based on ITU-T X.805 and NGN safety threats and vulnerability analysis[6]. NGN protection measures are selected to identify. Since network characteristics such as risk and vulnerabilities can be related to each security aspect, network attributes such as vulnerabilities and threats may calculate the degree to which NGN security objectives are achieved. A three-dimensional protection metric model is built, based on the above discussions[2]. The nature of protection is the ongoing playing with security vulnerabilities between the attack side and defence side and also the effort of both parties to achieve their goals by identifying vulnerabilities. The vulnerabilities in NGN’s network design, network components, protocols, and security management issues are analyzed[13][27].

A. Network Design Considerations:
One key element of NGN is that it should be an architecture for open systems. It supports access for multiple types of applications, like GSM, GPRS, 3G or POTS, wireless Internet and Wire-line. And all sorts of gateways connect trustful internal networks and unreliable external networks[13]

B. Network Components:
All unattached physical infrastructure entities, including all communication equipment, NGN core components, net management equipment, and all operator terminals and OM devices are known as network elements (NEs).
C. Security Management:
Administrators play an important role in network security, as the network management level can directly affect the security of the entire system. NGN should meet different security needs while using different security strategies as a convergence of a trustworthy network and incompetent network, which creates a major problem for network security management. With this, the need for application-level security can be brought up, which needs to check for anomalies.
Each layer on structural layers has the normal features of each layer and every layer also has its own vulnerability and threats. Once three layers have been identified, three models have to be considered for each one of the three protective layers. Privacy plans (Fig. 8) show network behaviours [13][28]. To counter the attacks on a wireless network a plan was proposed by Masoud Hayeri Khyavi et. al. in their research
• End Users Security
• Control Security Plan
• Management Security Plan

IX. A NEW SECURITY APPROACH

This solution is proposed to make the network of the next generation safer and more focused on practical applications[13]. The project is being explored in this process, in particular, a The protection and vulnerabilities, threats and protection viewpoints In three applications programmes, risks and future threats Areas: management, management and end-users, defined and He learned. Learned. At this point, one of the most critical problems An information security control framework is necessary Network and service providers correspondence. This outcome returns to dynamic value and advantages the information security system’s potential and After each stage of the new production is completed New preventive or reactivation experience will be Thinking. Thinking. Weaknesses, challenges and hazards of this framework Each scheme and its effects can be described and The hazards and risks in their analysis can be established. This network. The network.

A. Identifications:
During this stage, the project is investigated in particular from a safety point of view and the vulnerabilities, risks, threats and potential threats of the application services are identified and studied in three areas: management, monitoring, and end-users. A network security monitoring system for network communications and service providers at this stage is one of the most important issues. The significance and value of this outcome are expressed in the complex capacities of the information security system and the new knowledge and preventive and reactivation are considered after completion of each phase of the production[6]. This program will identify the failures, threats and risks of each scheme and identify the threats and risks of the network from the results and their analysis[13].

B. Plan and Resolution:
Essentially two steps are proposed
1) **Design and Planning:** For security software programs based on comprehensive network policy, the following policies must be provided during this phase by using documents, outputs and results in the previous stage:

- Business and corporate security policy
- Policy for application control
- Policy for end-user authorization
- Policy for cybercrime and forensics

2) **Presenting a Solution:** In this step, the best outcome would be identified and two implementing plans would be created with respect to the chosen policy and the use of related criteria, guidelines, logistics and necessary tools[1]. The security solution offered in the short-term plan will be inserted into the next generation network application layer as a bundle of proposals (serum systems). The proposed long-term implementing the plan will be implemented, with testing and feedback [13]. Short-term system outputs and input effects create a tailored long-term plan. This plan will create, evaluate and prioritize the implementation of new technology [3], its safety considerations, the optimal risk management and removal of existing security vulnerabilities within the time frame and policy that is suitable for this area.

**X. Discussion**

Wireless networks are important and used for several purposes [29-32] and it can be fit in any domain of application including health critical applications. However, its security [33-35] has higher concern, and it is not easy to manage, due to the form of this network, and due to implementation in several domains as well. This technology normally boosts the use of other cutting-edge technologies, such as 5G [36] Cloud, and higher data transfer other wireless applications. This concludes that the use of wireless network is vast, and it is highly beneficial as well. However, at the same time the concerns related to its energy efficiency and security are there as well.

**XI. CONCLUSION**

For a limited time, safety measures would be successful if the future state was not expected. Making every field secure would be such a puzzle and playing chess, in particular in the communication network, which puzzles items in each phase change, and the competitor is clever enough to take advantage of any wrong move. Designing and improving such processes and procedures is an additional network safety tool that will be necessary especially for the prediction and adoption of prevention activities as well as a response to security threats in the next-generation networks. By compromising its credibility and improving the development of new technologies and system performance and complexity, NGN needs a security framework over time. NGN will not hesitate to implement new technologies. This element of two mentioned models can manufacture a software, hardware, security and human interconnection intelligence system. This model positions the network security framework standby, which allows network intruders and cyber accidents to be ready. All malware is monitored from the beginning of access to NGN and a specific and technical safety research environment is prepared.

All in all, we are audacious about the reliability of wireless networks! While all vulnerabilities in Wireless Networking can be difficult to eradicate, overall security is rather easier to achieve if a systemic method for evaluating and managing the risks is adopted. WLAN users must therefore constantly take advantage of the steps outlined in this paper to defend against potential risks. However, adequate safety knowledge, accurate implementation and continued maintenance are a notable best practice for the securement of the wireless
REFERENCES

[1] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[2] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[3] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[4] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[5] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[6] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[7] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[8] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[9] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[10] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[11] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[12] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[13] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[14] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[15] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[16] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[17] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[18] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[19] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[20] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[21] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[22] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[23] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[24] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[25] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[26] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[27] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[28] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[29] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[30] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[31] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[32] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[33] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[34] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[35] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[36] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[37] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[38] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[39] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[40] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[41] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[42] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.

[43] Techopedia; "Techopedia explains Wireless Network"; https://www.techopedia.com/definition/26186/wireless-network;

[44] Edward Tetz; "Wireless Networking Infrastructure"; https://www.definitions.com/programming/networking/cisco/wireless-networking-infrastructure-mode/.

[45] Gigamon Blogs; "What is Networking Infrastructure?"; https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure.

[46] Pooja Rani, Kavita, Sahil Verma, Nhu Gia Nguyen; "Mitigation of Sybil Attack Using Wireless Sensor Network"; International Journal of Computer Science Issues, Vol. 7, Issue 3; https://www.ijcsi.org/papers/7-3-11-23-27.pdf

[47] Rehman A., Rehman, S.U. Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 86 (2017) 2291–2313 (2019). https://doi.org/10.1007/s11277-018-0960-7

[48] Aykut Karakaya, Sedat Akleylek; Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks; 978-1-5386-3449-3/18.

[49] IOP Publishing; "IPv6 Security - An Overview"; https://phoenixts.com/blog/types-of-wireless-network-attacks.
[30] Zaman, N., Low, T. J., & Alghamdi, T. (2014, February). Energy efficient routing protocol for wireless sensor network. In 16th International Conference on Advanced Communication Technology (pp. 808-814). IEEE.

[31] M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, “Emerging Smart Logistics and Transportation Using IoT and Blockchain,” in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 58-62, June 2020, doi: 10.1109/IOTM.0001.1900097.

[32] Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2020). Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Personal Communications, 1-22.

[33] S. J. Hussain, U. Ahmed, H. Liaquat, S. Mir, N. Jhanjhi and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/ICCISci.2019.8716471.

[34] Alsade, F., Zaman, N., Abdullah, A., & Dawood, M. Z. (2012). Enhancing Surveillance and Security of Oil Pipelines Transportation Using Wireless Sensor Network. Middle-East Journal of Scientific Research, 11(8), 1029-1035.

[35] Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z. Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, Ad Hoc Networks, Volume 101, 2020, 102096, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102096.

[36] Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588.