An Adaptive Auto Incident Response based Security Framework for Wireless Network Systems

Sindhu N Pujar[1], Gaurav Choudhary[2]*, Shishir Kumar Shandilya[1], Vikas Sihag[3],
and Arjun Choudhary[3]
[1]School of Computer Science and Engineering (SCSE), VIT Bhopal University, India
[2]Department of Applied Mathematics and Computer Science,
Technical University of Denmark (DTU), Denmark
[3]Department of Cyber Security, Sardar Patel University of Police, Jodhpur, India
sindhu.n2018@vitbhopal.ac.in, gauravchoudhary7777@gmail.com,
shishir.sam@gmail.com, vikas.sihag@policeuniversity.ac.in, a.choudhary@policeuniversity.ac.in

Abstract

The growth of wireless network systems is expanding deploying techniques to drive more network capacity and enabling low device complexity with low energy consumption to improve Quality of Service also a proper balance between data transmission and data integrity. Market Growth of Wireless Network System is expected at 62.8 million USD and is likely to grow at a CAGR at 17.5% to reach a valuation of 95.3 billion USD in 2024. Market grows significantly due to demand for network infrastructure and advancement in Artificial Intelligence (AI), Machine Learning (ML), and Big Data Analytics. The economy focuses on developing communication between network devices for ensuring secure communication using wireless systems. The nodes of network systems have limited power capacities where some batteries are chargeable or non-rechargeable by influencing the power of network system we can increase the performance of the wireless network system. These systems are generally susceptible to failures and attacks so it is necessary to impose stringent countermeasures on data integrity, data reliability, the transmission of data through network traffic in critical infrastructure. In this paper, we have proposed a model which is well suited for wireless network systems and devices to identify, detect, categorize and respond to attacks which in turn will generate warnings and alarms in case any malicious activity is observed. Implementing and deploying a model to effectively respond to incidents, selecting response actions for ensuring better protection of wireless network systems with the help of the AES encryption method. The system also integrates into generating warning messages and alarms/alerts raising concerns upon detecting or identifying any kind of intrusion.

Keywords: Incident Response, Security Framework, Wireless Network System, Risk Management

1 Introduction

Wireless Network Systems is expanding rapidly adopting a wide range of applications for security purposes, automating incidents, and monitoring them. These Wireless Network Systems monitor network traffic to check for audit logs and detecting malicious scripts entering into a secured network which may harm the environment creating a disbalance in a secured network system. Enabling technologies or wireless communications which are feasible, cheap, and tiny in order to deploy them in-network through wireless links. According to the recent trends, the wireless network security would register a CAGR of 12% over the period. The increasing population now adapts to wireless communications or network

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 4 (August 15, 2021)
DOI:*10.22667/ReBiCTE.2021.08.15.004*

*Corresponding author

systems in both residential and commercial space to augment the demand for Wireless Network Security. According to Wireless Broadband Alliance, (WBA) 90% roll out Wi-Fi6 and 66% are planning to develop next generation. Wi-Fi Hotspots are estimated to increase by 628 million, growth in Wi-Fi is directly proportional to security risks increasing which require adopting robust encryption.

Wireless Network Systems have come up with many advancements in the field of security, even though there have been incredible advancements in wireless systems it has not taken modern civilization to a level where it has to reach in a short span of time but is still making other developments.Smartphones, microchip technology, tablets, and GPS are the advancements of the Wireless Networks Systems. Mobile Edge Computing has rapidly taken place in the digital world, offering products and as-a-service offerings [14]. IoT Applications compute processing and storage which stores information [3, 37]. Spectrum Sharing is another trend that is brought into action recently but is limited to roll out 5G services [4, 16]. Capabilities are offered to Wi-Fi standard for better battery life which will increase performance and reduce the cost of energy optimization and simultaneous connections to the single access point. Open Wi-Fi networks project malicious intent also few people are able to secure networks [19]. Issues with wireless networks are that people come across a connection where they get connected after an establishment and verify if it is Wi-Fi before connecting because hackers sometimes may name the networks in a way to impersonate themselves as a known network in order to attract more people to connect to the network and steal the information of people.

Security Architecture of Wireless Network System integrates numerous mechanisms and countermeasures for protecting network traffic [11,12]. Security is integrated for a secure network system where at some point they can become a point of attack [8,22]. Effective incident response requires professional security teams to remediate threats, attacks, respond to issues immediately in absence of human, robust procedures to address issues without impacting other operations taking place simultaneously generating warnings, monitoring alerts, managing infrastructure is a very crucial thing. Deploy proper IRS and security mechanisms to secure data, as data is transferred through network traffic via network packets. The intervention of humans adversaries isn't recommended, as they attempt to compromise the network. Security systems are to be more secure to ensure protection against vulnerabilities [32]. Lack of energy and storage most mechanisms are not effective and approaches may not be feasible at times [16]. On reviewing various protocols, classify the security issues based on severity also outlining security constraints to present future directions based on emerged application fields [34].

1.1 Problem Statement and Our Contribution

Advancement in electric and electronics has made wireless communications grow rapidly, these technologies have made it possible to build small devices and deploying in network systems to check for malicious activities and monitoring wireless networks. Due to inherent and constrained resources security in WNS pose different challenges various security issues mostly affect performance in WNS, Energy, Hardware and Software Issues, Robustness, Fault Tolerance, and Physical Attack Security. Researchers have proposed Witness-based Detection Forwarding Misbehaviour's, Traffic Surveillance and Management System for WNS, Self-Managing and Self-adaptive Intrusion Detection System, Fault-Tolerance System and many more. Wireless Network Systems must implement Cryptographic Algorithms in constrained networks for improving energy consumption of network nodes, lack of physical security, low detection and false positive rate, Quality of Service (QoS), the establishment of encryption protocols. Propose new security protocols to make a balance between QoS provided by solutions and also respecting the limitations by network nodes. We Proposed a generalized solutions to raise and trigger alarms in network traffic, generate warning messages to the neighboring network, establishing protocols for physical layer security, detecting anomalies, enhancing the security of WNS.

2 Related Works

This section focuses on approaches for Wireless Network Systems which automate incident responses and ensuring security to the wireless networks as these networks are on the rise nowadays, we discuss works related to managing or handling incidents inside Wireless Networks or review the existing work that has been implemented so far. Wireless Technologies/Communication has a huge impact in the field of healthcare these technologies prove beneficial for data collection, portability, increased productivity, and lower installation costs. The state of the art solutions of auto Incidence response in Wireless network security is shown in Table 1.

Asim et al. [1]. have proposed an approach discussing dealing with incidents that occurred in the wireless networks and proposed a fault model which detects incidents by monitoring wireless networks. This model will also work on various network layers to automate response in cases of malfunctions. In this approach the efficiency of managing incidents is high they also proposed a method that tracks the impact of the incident over the wireless networks. Pervez et al. [27]. builds a strong fault-resilient wireless-based response system to execute operations that handle incidents at the time of fault occurrences. Hasswa et al. [10]. discussed building a response system into the wireless ad hoc networks which establish a response mechanism to discover malicious nodes caused by DOS, packet flooding, etc., and employing a watchdog that will notify of any malicious activity taking place in the network systems. For most Wireless Networks, it is important to scrutinize the networks to respond to security threats where these alerts can be effectively handled without any human intervention. The proposed models have discussed approaches to respond to threats and incidents immediately as soon as they're discovered but in all of the contributions described they lack in reporting the weaknesses to the security teams of the organization even if the system responds to the weakness at that very moment, it is also necessary to report the issues to the security team to find ways to mitigate them and also in minimizing the attacks.

Elmrini et al. [6] and Pervez et al. [27] have listed various application areas of Wireless Network Systems and focusing more on Network Traffic Data, it is a large-scale deployment of network monitoring systems. These systems depend on intrusive sensors which have many features also the advantage of monitoring network traffic in wireless networks is much effective way as it the most accurate sensor network giving accurate results, they are cost-effective, authors have also discussed maintenance, flexibility, and wireless communications in wireless networks. The author Elmrini et al. [6] have also proposed subsystems for managing network traffic with the help of data acquisition subsystem and control and data subsystem. In this paper, the authors have mentioned the performance of wireless technologies in different devices such as Bluetooth, ZigBee, WiMAX, LoRa, UWB, 3G/4G Technology where they analyzed the devices based on performance metrics. The authors have also discussed the application areas of wireless technologies in real-time scenarios and listing various response systems that are built which are used in various sectors. The main objective of discussing applications of Wireless Networks Systems is to give a brief description of response systems and their importance in Wireless technologies. Other networks like ad hoc mesh networks which are self-managing and self-organizing networks which are used to respond to incidents. Also discussing how hybrid networks use satellite technology used to execute emergency-related activities.

Fault Detection in Wireless Network System is a must it checks for risks or faults which are prone to cause damage to the network and other related devices or systems, the WNS is computing algorithms used for monitoring various environments including remote and geographical regions [17]. Asim et al. [1] presented techniques to recover and diagnose faults found in WNS also giving a brief comparison of fault models with the existing ones where the author considers a need to address a general fault model which not only focuses on individual node level but also considers network and management aspects. Fault detection and recovery are a critical issue that needs to be addressed as any kind of intrusion from

Table 1: The state of the art solutions of auto Incidence response in Wireless network security. (P1-Self-Managing Response Systems, P2-Applications of Wireless Network Systems, P3-Fault Detection and Recovery Response System, P4-Security Issues and approaches of WNS, P5-Anomaly Intrusion Detection in WNS, P6-Challenges in Wireless Network Systems)

Authors	Key Contributions	P1	P2	P3	P4	P5	P6
Asim et al. [1]	Proposed a fault management mechanism to deal with fault detection and recovery	Yes	No	Yes	No	No	No
Pervez et al. [27]	Implementation of Emergency Response Systems in Wireless Technologies and its Applications	Yes	Yes	No	No	No	No
Hasswa et al. [10]	Proposing a novel model for Intrusion Detection and response System for WNS to discover malicious nodes	Yes	No	No	No	Yes	No
Elmrini et al. [6]	Proposing set of countermeasures in order to avoid congestion and improve the flow of traffic	No	Yes	No	Yes	No	No
Xiaojiang et al. [5]	Paper has done comprehensive research on security of Wireless Network Systems focusing on issues and security schemes	No	Yes	No	Yes	No	Yes
Jianqing et al. [21]	Proposing three-logic-layer architecture for Intrusion Detection System which self-configures issues or incidents inside WNS	No	No	Yes	No	Yes	Yes
Sultana et al. [33]	Emphasized on security approaches of WNS and also focuses on developing Network Model to automate response for anomalous behaviour in WNS	Yes	No	Yes	No	Yes	No
Pathan et al. [26]	Focused on investigating Wireless Network Security and proposed holistic security approach to deal with challenges in network system	No*	Yes	No	Yes	No	Yes
Sharma et al. [31]	Providing overall insight in the field of Network Security in Wireless Networks and exploratory summary of the challenges	No	Yes	No	Yes	No	Yes
Falcon et al. [7]	Proposing Multi-modular,real-time risk-management framework for Wireless Network systems which features evolving shadowed clustering architecture based on fuzzy risk assessment	No*	Yes*	No	No	Yes	Yes*
Kim et al. [15]	Discussing on various mechanisms proposed by authors for Wireless Network systems which also proposes of developing a Diffie-Hellman Algorithm	No	Yes	No	No	No	Yes
McCoy et al. [23]	Discussing on various mechanisms proposed by authors for misbehaving nodes in wireless network systems	No	Yes	Yes*	Yes*	No	No
Koushanfar et al. [18]	Proposing techniques on fault-tolerance in WSN and comprehensive study on levels of abstractions	No	Yes	Yes	No	No	No
Lee et al. [20]	Comprehensive study on applications on wireless networks in various fields and also discussing of encryption algorithms for different network systems	No	Yes	No	No	No	No
Rajadurai et al. [30]	Proposed Stacked ensemble intrusion detection model for evaluating the performance different ML algorithms which will also depict accuracy of model helping us in choosing best algorithm for model	No	Yes	Yes	No	No	No
Hämäläinen et al. [9]	Paper presented implementations and design of 8-bit AES encryption for low-cost and low-power devices	Yes*	Yes*	Yes*	No	Yes*	No
Othman et al. [25]	Paper has discussed of AES encryption methods also measuring and comparing its energy and consumption in networks.	No	Yes	Yes	No	No	No
Ragsdale et al. [29]	Paper proposed prototypes of Intrusion Response Systems to detect and respond to sophisticated attacks.	Yes*	No	No	No	Yes*	No

a third party or security breach may cause damage to the device. Moreover, the author also proposed solutions to perform fault detection and fault diagnosis with the help of proposed algorithms for better accuracy in detecting and diagnosing faults in wireless networks.

2.1 Wireless Network Security

Security of Wireless Networks is a critical thing to address or in other words we can say that security of these networks is what we have to majorly focus on as ensuring protection of data and by restricting access points to public networks can minimize the risks to wireless networks. In this paper, Xiaojiang et al. [5] has proposed various issues formulated in the wireless networks and also elaborating on various protocols and techniques to be incorporated by the wireless networks. The author [13] also surveyed on large-scale wireless networks as to how they are susceptible to attacks and the impact or the intensity of the attack to the network system which is likely to cause damage to the system. The author has listed few defense techniques to mitigate the risk of compromising the security in different network layers such as Physical Layer (Jamming and Tampering), Link Layer (Collision, Manipulating Routing Information& Exhaustion), and Network Layer (Sybil Attack and Selective Forwarding Attack).

Approaches discussed by Xiaojiang et al. [5] are the different schemes proposed for network servers and sensor nodes to maintain CIA. The author has also come up with a concept of secure routing discussing efficiency and issues caused by this mechanism in securing the wireless networks. A positive contribution of the approaches and issues is they have proposed establishing these schemes and techniques for low-cost, energy-consuming systems, small-size sensor nodes in large-scale sensor networks. The author [2] has primarily focused on discussing the protocols and schemes but they haven't discussed reporting the issues found with these mechanisms in case anyone faces issues with the schemes and there are adversaries which can harm the network system so steps or techniques to mitigate or emergency reporting system should have been implemented to safely secure the environment.

2.1.1 Anomaly Intrusion Detection in WNS

Jianqing et al. [21] has proposed an IDS architecture for the three-layer network which deploys a self-adaptive approach for self-configuring or detecting incidents inside the wireless network with the help of work modes as discussed by the authors are active work mode and passive work mode for known and unknown attacks but the accuracy for detecting anomaly attacks, they have also proposed intrusion detection mechanisms for local intrusion detection systems as well. The author has focused on three factors to secure wireless networks the incident response, intrusion detection, and evolution approach by developing a self-adaptive system to analyze and deploy attacks in WNS. Sultana et al. [33] has implemented viable solutions to deploy and detect attacks in IDS and proposed an approach to security incident response and prevention systems for different application areas in wireless networks systems which will generate a response to anomalous behavior of network nodes.

A watchdog monitor is also developed by the authors of this paper to keep a watch on the network traffic for surveillance of different kinds of attacks. The positive contribution of the author towards this approach is they have discussed employing emergency response systems and generating responses to network incidents and setting up a surveillance system to track irregularities of the network system and real-time monitoring, also they have generated a model to filter and diagnose adverse events occurring in the wireless network systems [35]. The drawback of the proposed architecture or the model they can also combine another factor to generate warnings or raise alarms on any malicious activity which is detected or discovered in the system. Also maintaining high accuracy for detection and filtration of adversaries is necessary which has to be improved and effective action against such anomalous behavior.

2.1.2 Challenges in Wireless Network Systems

Wireless Network Systems have great potential they can expand our ability to monitor and interact remotely with the physical world. The sensors of the wireless network system have the ability to collect a huge amount of unknown data. For Wireless Networks to be ubiquitous a lot of challenges must be overcome. The major challenge in wireless networks is to detect and diagnose newly found and unknown attacks which will require time in understanding the pattern of the attacks and the impact this attack can cause if security is compromised in any way so in this paper Pathan et al. [26] has done a comprehensive review in understanding the security issues of the wireless networks in order to improvise it and also proposed about developing a holistic security approach mechanism that detects false reports.

The author has also mentioned that different systems perform different tasks as there is no combined effort for creating a common model for all the mechanisms to be included to provide a common platform to perform all the tasks required when any attack or incident occurs in a wireless network. Their positive contribution towards this is the authors have discussed various schemes to be proposed for the wireless network systems to increase the accuracy of detecting and handling an incident without any human intervention. The author has also discussed routing algorithms to secure the network system and fight against black holes inside the network. Sharma et al. [31] has done extensive research in understanding various kind of challenges in Wireless Network Systems by citing issues that affect the design and performance of the network system such as Energy, Self-management, Hardware and Software issues, Security, Deployment, Fault Tolerance, OS, MAC Layer Issues, Data Collection and Transmission, etc.

3 Auto Incident Response in Wireless Network Security

Wireless Networks have been on the go nowadays, there is also a need for effective security mechanisms. As these networks continue to transmit sensitive data so it gets difficult to address security issues from the beginning of system design. Wireless Networks transmit data packets to the destination via intermediate nodes in the network. To establish a secure connection within networks and ensuring that packets transmitted from one node to the other end of the node have to be secured in order to prevent any kind of malicious activity taking place or misbehavior in the network. Deployment of secure routing protocols in [36], defense mechanisms, generating an alarm to notify network, raising warnings with respect to attacks detected. Due to inherent resource and computing constraints security in wireless networks poses different challenges [7] [26] than traditional network security. Unlike, traditional networks sensor nodes are often deployed in large accessible areas which also adds the risk of physical attack. As and when these wireless networks are in communication with people there is a risk of new security problems arising every day. With this in mind, wireless network system security presents obstacles and requirements for a resilient security profile.

3.1 Security Requirements in Wireless Networks

When information is transmitted from one node to another in Wireless networks which are exchanged among authorized users, it may be vulnerable to malicious threats that owe to the broadcast nature of wireless medium [28]. The wireless networks have some major security requirements that have to be fulfilled and some of them are mentioned for protecting wireless transmissions against wireless attacks like eavesdropping attack, DOS attack, data falsification attack, node compromise attack, etc. There are few security requirements of authenticity, confidentiality, integrity, and availability

- Integrity: To maintain integrity many security protocols are deployed and also follow security policies. It is also necessary to enable sensor nodes to detect modified, injected, or replayed packets as an attacker sends any false messages the receiver ensures that data used in the decision-making process is valid [33]. There are mechanisms to instantiate common security functionalities for identification and remediation of devices engaging in misbehavior, which is Misbehaving Node Detection Mechanism designed to provide a policy-based mechanism and can remediate nodes that violate policy This is also robust to malicious attackers [23].

- Authentication: There are mechanisms developed were sending and receiving nodes share secret keys. As the media has wireless nature which may cause data loss or damage then it becomes challenging to ensure authentication. These mechanisms mainly focus on securing the network and using these techniques it is possible to detect compromised nodes. The DICAS protocol is developed to detect malicious nodes in multi-hop wireless networks. This also includes neighbor discovery and authentication algorithm enabling nods to route around malicious nodes which are authenticated. Wireless networks like ad hoc networks use authenticated nodes using public-key authentication to ensure that each node in the wireless network has a valid public/private key pair. Mechanisms are being developed for compromised authenticated nodes.

- Confidentiality: It can conceal network traffic from the passive attacker; any message communicated through wireless networks remains confidential. This is also considered an issue in network security. Applications like key distribution the nodes communicate highly sensitive data. The Standard approach [20] of confidentiality is to protect the data using key encryption methods and establishing public-key cryptography methods but are expensive to be used in resource-constrained wireless networks, most protocols use symmetric key encryption methods. Security of communications inside wireless networks is assured and it doesn't prevent the misuse of information reaching base station [23]

3.2 Risk Management For WNS

An architecture model is proposed for risk management was risks are categorized as the wireless network system monitors. This framework splits multiple discrete snapshots to capture structural dynamics in real-time data in a wireless network system. In the era of digital technology, it is bound to have threats and risks for any kind of communication we use, proliferation of technologies and devices has given benefits and opportunities but it also exposes us to various kinds of risks. [18]As and when the technologies or devices get advanced every day even the complexity of mitigating and detection of the risks or threats become challenging which are mostly associated with wireless network communications. Many wireless networks are targeted through network layers in OSI Model as discussed here [24].

Management of these risks and exploits which are vulnerable to attacks, these things are considered in order to mitigate them or prevent them security assessments has to be performed prior to developing any kind of wireless device or technology. Security policies have to be in check on a regular basis which would recognize the threat levels and impact of damage it can cause. Implementing different mechanisms or models for generating automated warnings or alarms in wireless networks in Traffic Surveillance [6]with the help of the Master-Salve paradigm in linear topology it has many sensor nodes which are used to manage such risks and protecting the surveillance system by mitigating it. A risk management framework is proposed for wireless network systems which capture multiple risk features and also provide a visual depiction of corporate network threats at any time and numerical assessments of the sensor's overall risk. Risk assessment embraces fuzzy and shadowed evaluations of risk sources and incorporates an adaptive learning process that weights risk sources proportionally to their observed impact on failed sensors, the framework is highly automated and human-centric in nature.

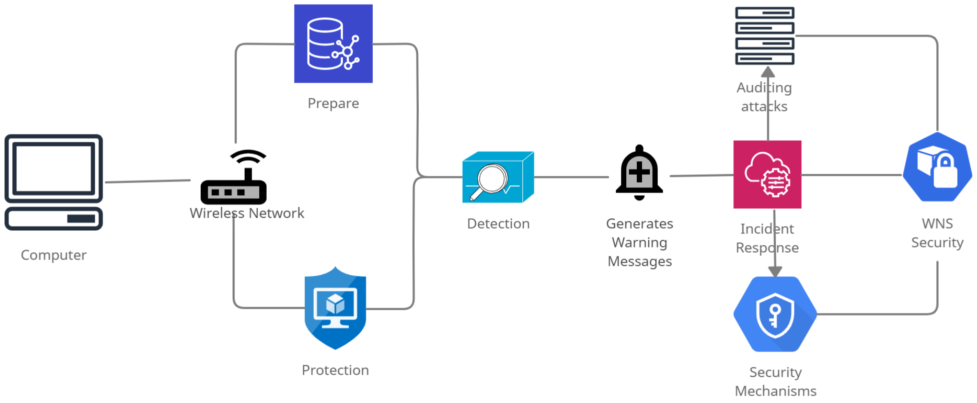

Figure 1: The Work Flow of WNS.

3.3 Countermeasures In Wireless Networks

There are constraints specified for wireless network systems which expose them to various threats and vulnerabilities. In ad-hoc networks, they're specific to wireless networks and are designed to deal with exploits or vulnerabilities. Attacks are classified based on passive/active attacks, internal/external attacks where a node in the networks is involved in the network and can also be achieved by deploying nodes in a wireless network that are captured physically [33]. If the node is involved in an attack inside the network, and then it's external. Attacks like a sinkhole, selective forwarding, black hole, wormhole attack, performed on data packets for false data injection, and delayed forwarding is conducted to degrade data quality and utility. Sybil Attack is mostly done for tampering or physical capture of data packets in network data traffic but is also adversary as they extract sensitive information from the data packets, these attacks are implemented by enabling the malicious node to present multiple identities to the network, do not automate response actions with respect for such kind of attacks. The analysis is carried out to initiate remedies in WNS for the attacks.

Contributing to these mechanisms by deploying low severity actions in wireless systems and devices for monitoring network traffic where precise attack detection is done and does not give out erroneous responses and preserving WNS services when any failure or attack takes place. To recover from them and prevent malicious attempts the severity responses are generated by those local sensor devices to execute it. Firewalls are a great option to secure the wireless network systems, it checks data packet and decision making is done for rejecting or accepting the packets. It is a security device that monitors incoming and outgoing traffic and decides whether to allow or block depending on security rules [6]. Reducing the risk of DOS attacks by performing routine audits on wireless network activity and performance will identify the problems. Creating a DMZ subnet is used to improve security by segregating computers on each side of a firewall. The Work Flow of WNS is shown 1.

4 Proposed Solution

In this section, we have deployed a model for the Wireless Network to respond to incidents and also ensuring security to the devices/networks and also begin with discussing the various cryptographic encryption algorithms and implementing a model for automating responses in Wireless Network Systems as automation of intrusion detection system is very limited, the process for this includes detection of attacks, security of wireless networks and user information, improving the performance of few crypto-

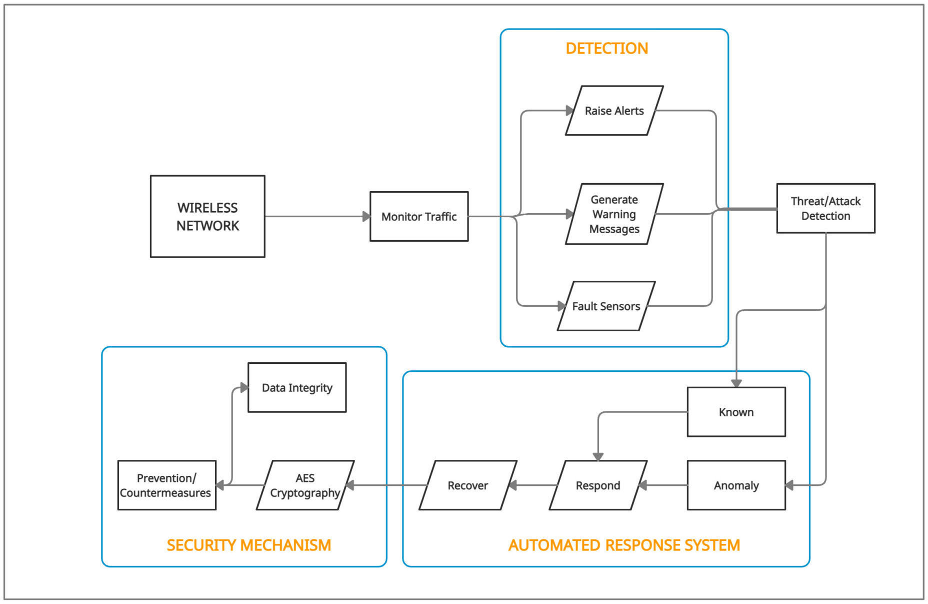

Figure 2: The wireless Network Model.

graphic algorithms.

4.1 System Model

Wireless Network System is for automating responses for any kind of suspicious activity or network attack detected and to ensure security protocols are followed by the system keeping data integrity in check, to do so a device is required to monitor network traffic for detecting anomaly-based attacks or known attacks. The model will also deploy security algorithms and protocols to ensure stronger security to the wireless network systems to keep data integrity in check. The model will store log data to keep a record of incidents and the model will automate response systems depending on the detection of threats or any suspicious activity.

The model comprises of Detection Phase, Response System, and Security Mechanisms.

- Detection Phase

  Wireless Network is continuously monitored to check for malicious activity recorded or predicting for any such activity that may take place in the future depending on security failures experienced by the system, then the detection phase will scan and classify the attacks based on the risk levels and identify if the attack is known or anomalous. After detecting the attack system will then generate alerts, warning messages and also sense the fault causing the attacks.

- Incident Response System

  In this part system provides immediate response to the detection through an automated process where intrusion detection system is automated as soon as an attack is identified, the response system will respond to the attack as it is integrated with the detection system to identify the source of the attack and recover the attack occurred immediately it is identified.

- Security Mechanisms

The final stage comes where we secure the network between users or any other wireless communications to ensure that security isn't breached the response system is associated with the security phase to deploy automatic countermeasures to monitor traffic continuously. To ensure stronger security inside network traffic implementing AES Algorithm for encryption of data and to avoid any data loss to insider attacks or malicious activities.

4.2 Implementation

Intrusion Detection System is known to be a secure defense of network for Wireless Network Systems as the systems are advanced nowadays and traditional IDS won't work with these kinds of systems, deploying a detection system such that it classifies the malicious attacks, monitors the network traffic to collect information on the suspicious activity or abnormal behaviors in the wireless network, it also monitors events to taking place in network traffic to identify intrusions [30]. IDS system will generate warning messages and raise alerts. It is most helpful for anomaly detection to monitor, generate alert/warning for abnormality and unknown attacks, signature-based detection for known attacks. This system will evaluate and analyze the threat levels caused by the detection of abnormalities or attacks found with the help of a clustering model, forming clusters of threats found based on risk levels and classifying them on the basis of attacks; known or unknown attacks.

The response system will be integrated with the detection system to further proceed with the automating responses to incidents identified. Deploying static-based response system where it uses signature-detection and anomaly detection for suspicious behavior in wireless networks. It is necessary to implement a response system by automating the actions to respond and recover the attacks, they are essential for responding to potential intrusion and attacks these types of response systems are beneficial as they do not require any human involvement to respond to the attacks or abnormalities. It will also reduce the time delay for responding to attacks whenever any malicious activity is identified. They monitor wireless networks to effectively recover the network and address potential incidents. With the help of automating responses to incidents in wireless network traffic, it must have countermeasures prepared to avoid such abnormality in the future.

AES algorithm is a block cipher having low complexity also has high-level security and also has a crucial role in encrypting confidential data by storing it in insecure networks where it is not accessible by unauthorized attackers so they can't read it. The input block will have to continuously go through the transformation before giving the output. Apart from this the phase will not only encrypt the sensitive data but will also provide countermeasures to the wireless network to mitigate the risks or any kind of suspicious activity. It is mainly provided by the Response system phase. Data integrity is implemented with the help of the AES Algorithm.

4.3 Discussions

The Wireless Network System will be deploying an AES encryption algorithm for securing data and also implementing the algorithm to secure the wireless networks from any kind of malicious activity taking place. Table 4.3 shows a comparison between various encryption algorithms and to get a better understanding of a secure method to implement in the system. DES cipher is known to be broken easily where it has known vulnerabilities, but AES is more secure than DES as it can encrypt 128 bits of plain text. Also talking about the techniques that these algorithms perform, the speed of CPU processing for encrypting and decrypting data is least in RSA as compared to AES CPU processes much faster than other encryption algorithms. Key generation is faster in AES than other algorithms, key size varies for different algorithms but AES being the highest among all which has 128-bit encryption to 256-bit encryption. AES, 3DES, DES uses symmetric block cipher whereas RSA uses asymmetric block cipher and also discussing the security in these algorithms it is known that AES has high-level security compared to DES, 3DES, RSA. With this, we conclude that using AES for encrypting data and also securing wireless networks is much effective and the performance of AES is higher.

Table 2: The state of art comparison of Cryptographic security solutions.

Features	AES	RSA	DES	3DES
Key Generation	128-bit, 192-bit 256-bit	depending on number of bits in modules	56 bits	168-bit or 112-bit
CPU Processing	Fast	Slowest	Slow	Very slow
Cipher Type	Symmetric Block Cipher	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Security	High-level Security	Least Secure	Adequate Security	Less Secure
Response Time	Faster	Slower	Moderate	Slow

5 Conclusion

In this paper, we have proposed a model which is well suited for wireless network systems and devices to identify, detect, categorize and respond to attacks which in turn will generate warnings and alarms in case any malicious activity is observed. The model has come across some challenges like performance and power consumption, Quality of Service affecting the accuracy of detection of attacks in network traffic which is then addressed by the intrusion detection system. The main goal is to identify faults, techniques for detection and diagnosis to ensure the efficiency of the mechanisms that will be adopted by the wireless network system. Failing to develop a secure model for the wireless network can lead to losing confidential data and the attacker may gain access to systems/devices that he wouldn't be if proper mechanisms were established.

In this paper we have also argued on the issues that exist in the development of WNS mechanisms and algorithms, evaluating every algorithm by the accuracy it provides and how secured the system is. Benchmarks are followed to solve experimentation issues, diagnostic issues based on the methods used in the paper. In any case, if these benchmarks are not resolved or any issues arise in the Automated Incident Response system then it may lead to poor detection and diagnosis of attacks, slow recovery, the performance of the intrusion response system degrades. A missed intrusion can result in severe damage to the system. False-positive indicate normal activities which were falsely detected as suspicious or malicious by the response system. An automated response system is deployed to identify compromised nodes, generating alarms in the system in case of any intrusion or false packets received. With this, we have come up with results by evaluating the response time of the encryption method used by other systems and our system where AES encryption is known to be the fastest and more secured method and consumes significantly less energy.

Future models should develop an advanced and effective model for detection and intrusion in wireless network systems, also improving the response coordination concerning critical and real-time incident response which will reduce data loss, improve quality of life and also save resources with effective deployment. We would also make use of advanced machine learning algorithms for diagnosing anomaly-based attacks in networks and developing an encryption method that would be more beneficial than the existing encryption method.

References

[1] M. Asim, H. Mokhtar, and M. Merabti. A self-managing fault management mechanism for wireless sensor networks. *arXiv preprint arXiv:1011.5072*, 2010.

[2] K. Chelli. Security issues in wireless sensor networks: Attacks and countermeasures. In *Proc. of the 2015 World Congress on Engineering (WCE'15), London, U.K*, volume 1, pages 876–3423, July 2015.

[3] G. Choudhary, P. V. Astillo, I. You, K. Yim, R. Chen, and J.-H. Cho. Lightweight misbehavior detection management of embedded iot devices in medical cyber physical systems. *IEEE Transactions on Network and Service Management*, 17(4):2496–2510, 2020.

[4] G. Choudhary and V. Sharma. A survey on the security and the evolution of osmotic and catalytic computing for 5g networks. In *5G enabled secure wireless networks*, pages 69–102. Springer, 2019.

[5] X. Du and H.-H. Chen. Security in wireless sensor networks. *IEEE Wireless Communications*, 15(4):60–66, 2008.

[6] A. Elmrini and A. G. Amrani. Wireless sensors network for traffic surveillance and management in smart cities. In *Proc. of the 5th International Congress on Information Science and Technology (CiSt'18), , Marrakech, Morocco*, pages 562–566. IEEE, October 2018.

[7] R. Falcon, A. Nayak, and R. Abielmona. An evolving risk management framework for wireless sensor networks. In *Proc. of the 2011 International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA'11), Ottawa, ON, Canada*. IEEE, September 2011.

[8] D. Fang, Y. Qian, and R. Q. Hu. Security for 5g mobile wireless networks. *IEEE Access*, 6:4850–4874, 2017.

[9] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen. Design and implementation of low-area and low-power aes encryption hardware core. In *Proc. of the 9th EUROMICRO conference on digital system design (DSD'06), Cavtat, Croatia*, pages 577–583. IEEE, August-September 2006.

[10] A. Hasswa, M. Zulkernine, and H. Hassanein. Routeguard: an intrusion detection and response system for mobile ad hoc networks. In *Proc. of the 2015 IEEE International Conference on Wireless And Mobile Computing, Networking And Communications (WiMob'05), Montreal, QC, Canada*, volume 3, pages 336–343. IEEE, August 2005.

[11] H.-D. J. Jeong, W. Hyun, J. Lim, and I. You. Anomaly teletraffic intrusion detection systems on hadoop-based platforms: A survey of some problems and solutions. In *Proc. of the 15th International Conference on Network-Based Information Systems (NBiS'12), Melbourne, VIC, Australia*, pages 766–770. IEEE, September 2012.

[12] C. Johnson, B. Khadka, E. Ruiz, J. Halladay, T. Doleck, and R. Basnet. Application of deep learning on the characterization of tor traffic using time based features. *Journal of Internet Services and Information Security (JISIS)*, 11(1):44–63, February 2021.

[13] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2-3):293–315, 2003.

[14] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage. A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, 22(1):196–248, 2019.

[15] D. S. Kim, S. Lim, and W. Zhang. Dependability and security for wireless ad hoc and sensor networks and their applications. *International Journal of Distributed Sensor Networks*, 9(7), 2013.

[16] J. Kim, G. Choudhary, J. Heo, D. G. Duguma, and I. You. 5g wireless p2mp backhaul security protocol: an adaptive approach. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):1–19, 2019.

[17] M. Kolomeets, A. Chechulin, and I. Kotenko. Bot detection by friends graph in social networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 12(2):141–159, June 2021.

[18] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli. Fault tolerance in wireless sensor networks. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, 2004.

[19] A. Kumar, S. K. Dhurandher, I. Woungang, and J. J. P. C. Rodrigues. Securing opportunistic networks: An encounter-based trust-driven barter mechanism. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 12(2):99–113, June 2021.

[20] J. Lee, K. Kapitanova, and S. H. Son. The price of security in wireless sensor networks. *Computer Networks*, 54(17):2967–2978, 2010.

[21] J. Ma, S. Zhang, Y. Zhong, and X. Tong. Said: A self-adaptive intrusion detection system in wireless sensor networks. In *Proc. of the 2006 International Workshop on Information Security Applications (WISA'06), Jeju Island, Korea*, volume 4298 of *Lecture Notes in Computer Science*, pages 60–73. Springer-Verlag Berlin Heidelberg, August 2006.

[22] S. Manipriya, C. Mala, and S. Mathew. A collaborative framework for traffic information in vehicular adhoc network applications. *Journal of Internet Services and Information Security (JISIS)*, 10(3):93–109, August 2020.

[23] D. McCoy, D. Sicker, and D. Grunwald. A mechanism for detecting and responding to misbehaving nodes in wireless networks. In *Proc. of the 2nd IEEE Workshop on Networking Technologies for Software Define Radio Networks (SDRN'07), San Diego, CA, USA*, pages 48–54. IEEE, June 2007.

[24] D. Mutakin, M. T. K. M. N. Khan, and J. Ibrahim. Cyber risk management for wireless communication in organization.

[25] S. B. Othman, A. Trad, and H. Youssef. Performance evaluation of encryption algorithm for wireless sensor networks. In *Proc. of the 2012 International Conference on Information Technology and e-Services (ICITeS'12), Sousse, Tunisia*. IEEE, March 2012.

[26] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong. Security in wireless sensor networks: issues and challenges. In *Proc. of the 8th International Conference Advanced Communication Technology (ICACT'06), Phoenix Park, Korea*. IEEE, February 2006.

[27] F. Pervez, J. Qadir, M. Khalil, T. Yaqoob, U. Ashraf, and S. Younis. Wireless technologies for emergency response: A comprehensive review and some guidelines. *IEEE Access*, 6:71814–71838, 2018.

[28] H. V. Poor and R. F. Schaefer. Wireless physical layer security. *Proc. of the National Academy of Sciences*, 114(1):19–26, 2017.

[29] D. J. Ragsdale, C. Carver, J. W. Humphries, and U. W. Pooch. Adaptation techniques for intrusion detection and intrusion response systems. In *Proc. of the 2000 international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions (ICSMC'00), Nashville, TN, USA*, pages 2344–2349. IEEE, October 2000.

[30] H. Rajadurai and U. D. Gandhi. A stacked ensemble learning model for intrusion detection in wireless network. *Neural Computing and Applications*, pages 1–9, 2020.

[31] S. Sharma, R. K. Bansal, and S. Bansal. Issues and challenges in wireless sensor networks. In *Proc. of the 2013 International Conference on Machine Intelligence and Research Advancement, Katra, India*, pages 58–62. IEEE, December 2013.

[32] V. Sharma, I. You, R. Kumar, and P. Kim. Computational offloading for efficient trust management in pervasive online social networks using osmotic computing. *IEEE Access*, 5:5084–5103, 2017.

[33] S. Sultana, D. Midi, and E. Bertino. Kinesis: a security incident response and prevention system for wireless sensor networks. In *Proc. of the 12th ACM Conference on Embedded Network Sensor Systems (SenSys'14), Memphis, TN, USA*, pages 148–162. ACM, November 2014.

[34] F. Ullah, M. Ahmad, M. Habib, and J. Muhammad. Analysis of security protocols for wireless sensor networks. In *Proc. of the 3rd International Conference on Computer Research and Development (ICCRD'11), Shanghai, China*, pages 383–387. IEEE, March 2011.

[35] T. Varshney, T. Sharma, and P. Sharma. Implementation of watchdog protocol with aodv in mobile ad hoc network. In *Proc. of the 4th International Conference on Communication Systems and Network Technologies (CSNT'14), Bhopal, India*, pages 217–221. IEEE, April 2014.

[36] S. Yang, S. Vasudevan, and J. Kurose. Witness-based detection of forwarding misbehaviors in wireless networks. In *Proc. of the 5th IEEE Workshop on Wireless Mesh Networks (WIMESH'10), Boston, MA, USA*. IEEE, June 2010.

[37] I. You, S. Kwon, G. Choudhary, V. Sharma, and J. T. Seo. An enhanced lorawan security protocol for privacy preservation in iot with a case study on a smart factory-enabled parking system. *Sensors*, 18(6):1888, 2018.

Author Biography

Sindhu N Pujar Sindhu N Pujar pursuing a Bachelor of Technology(B.Tech), Computer Science (specialization in Cyber Security and Digital Forensics) from Vellore Institute of Technology, Bhopal. She is qualified the NASSCOM Certification with Gold Level Certification. Her interest in research includes Threat Intelligence and Cyber security..

Gaurav Choudhary Dr. Choudhary received a Ph.D. in Information Security Engineering from Soonchunhyang University, South Korea. He has done a Master of Technology in Cyber Security from the Sardar Patel University of Police and received a Chancellor Gold Medal for Academic Excellence. He is presently working as a Security Researcher at DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU). Prior to joining DTU, he has also worked as an Assistant Professor in the School of Computer Science, University of Petroleum and Energy Studies (UPES), and School of Computer Science and Engineering (SCSE) at VIT Bhopal University. His current research interests include Threat Intelligence, IoT and CPS Security, Cyber Security, Vulnerability Assessment, 5G Security, Drone Security, and Cryptography. He has authored or co-authored many reputed SCI journal/conference papers and book chapters.

Shishir Kumar Shandilya Dr. Shishir Kumar Shandilya is the Division Head of Cyber Security and Digital Forensics at VIT Bhopal University. He is working as a Principal Consultant to the Cabinet Secretariat, Govt. of India for Technology Development and Assessment in Cyber Security. He is also a Visiting Researcher at Liverpool Hope University-United Kingdom, a Cambridge University Certified Professional Teacher and Trainer, ACM Distinguished Speaker and a Senior Member of IEEE. He is a NASSCOM Certified Master Trainer for Security Analyst SOC (SSC/Q0909: NVEQF Level 7) and an Academic Advisor to National Cyber Safety and Security Standards, New Delhi. He has received the IDA Teaching Excellence Award for distinctive use of technology in Teaching by Indian Didactics Association, Bangalore (2016) and Young Scientist Award for two consecutive years, 2005 and 2006, by Indian Science Congress and MP Council of Science and Technology. He has seven books published by Springer Nature-Singapore, IGI-USA, River-Denmark and Prentice Hall of India. His recently published book is on Advances in Cyber Security Analytics and Decision Systems by Springer.

Vikas Sihag Mr. Sihag has been an Assistant Professor with the Department of Cyber Security, Sardar Patel University of Police since 2013. He is also associated as a researcher with the Department of Computer Science and Engineering, National Institute of Technology, Raipur. He has received his Masters in Information Security from Motilal Nehru National Institute of Technology, Allahabad. His current research interests include Android security, malware analysis, digital forensics and protocol security. He is a British Standards Institution certified Information Security Management Systems - Lead auditor. He is also a CEH (Certified Ethical Hacker) and CEI (Certified EC-Council Instructor). He has organized various international and national training programs for Law Enforcement Agencies. He also has (co-)authored many journal/conference papers and book chapters.

Arjun Choudhary Lt. Arjun Choudhary has been an Assistant Professor with the Department of Cyber Security, Sardar Patel University of Police. He is Deputy Director at the Centre of Cyber Security, Sardar Patel University of Police, Security and Criminal Justice. His current research interests include Cloud Computing, Web apps, and Digital Forensics. He has organized various international and national training programs for Law Enforcement Agencies. He also has (co-)authored many journal/-conference papers and book chapters.