An Effectual Secured Approach Against Sybil Attacks in Wireless Networks

https://doi.org/10.3991/ijim.v16i09.30213

Sundresan Perumal(✉)
College of Information Technology, Islamic Science University, Negeri Sembilan, Malaysia
sundresan_197@gmail.com

Abstract—In both wireless and mobile ad hoc networks, assaults can come from a variety of different sources. The terms "active attack" and "passive attack" describe these two types of attacks. In the network community, the Sybil attack is one of the most often used and deployed techniques for sniffing identities and repurposing them. Multiple identities or Sybil attacks have recently sparked a lot of interest in the research community. The algorithms and networks on which they are tested are vastly different among the many methods that have been offered. Since researchers can't evaluate these systems side by side or test their efficacy on real-world social networks with a variety of structural features, it's difficult to say whether there are any other (perhaps more efficient) methods of Sybil protection. In the event of a Sybil attack, the gatecrasher subverts the system framework's notoriety arrangement by creating a large number of pseudonymous individuals and then using them to add an enormously imbalanced influence. Three factors determine a notoriety framework's susceptibility to a Sybil attack: how quickly personalities can be generated, how much the notoriety framework accepts inputs from substances that lack a chain of trust, and if the notoriety framework handles all components equally. A large-scale Sybil ambush in Bittorrent Mainline may be accomplished in a cheap and effective manner, according to confirmation. A substance on a distributed system is a piece of software that has access to the resources of the local community. By displaying a character, a distributed system element reveals itself to the world. A single chemical can have an impact on more than one character. Numerous characters can be assigned to a single element. The personalities of substances in shared systems are used for the objectives of repetition, asset transfer, reliability, and trustworthiness, among other reasons. For remote elements to be aware of characters without necessarily being aware of the personality-to-neighborhood correlation, distributed systems make use of the character as a decision. Each different identification is normally considered to be associated with a separate local entity by convention. A single local entity may have several identities in actuality. In order to avoid and identify Sybil assaults, an empirical technique is used in this study. According to the base paper, any nodes with RSS greater than the provided threshold are regarded to be attackers under the present approach. A centralized way to monitor the mobile nodes is required to prevent this assault. As the server agent assumes full control of the ad-hoc network, malevolent nodes or selfish nodes are fully eliminated from the system.

Keywords—network security, wireless network security, security in wireless environment

1 Introduction

A wireless sensor network (WSN) is a collection of geographically dispersed, self-contained sensors that work together to transmit data about physical or environmental factors, such as temperature, sound, and pressure, to a central hub. Sensor activity can also be controlled via the more recent networks, which are bi-directional. Many industrial and consumer applications now employ wireless sensor networks that were originally developed for military purposes such as battlefield surveillance; these networks are now used in a wide range of other applications [1]. Nodes in the WSN can range from a few to hundreds or even thousands, and each node is linked to one or more sensors. An electrical circuit for interacting with the sensors is normally a battery or an incorporated type of energy harvesting in a sensor network node. A radio transceiver with either an internal or external antenna is also frequently included. Shoebox-sized sensors to dust-grain-sized sensors are all possibilities for sensor nodes. But functional "motes" with really tiny dimensions have yet to be developed. Similar to sensor nodes, the cost of sensor nodes can range anywhere from a few dollars to hundreds of dollars per sensor node. Resources such as energy, memory, calculation speed, and communications bandwidth are constrained by sensor node size and cost [2]. An elementary star network to a sophisticated multi-hop wireless mesh network can be the WSN topology. Routing or flooding can be used to spread information across network nodes [3]. Wireless sensor networks (WSNs) are becoming increasingly popular as a low-cost means of keeping tabs on real-world conditions. Static nodes have traditionally been used to collect data from the environment via WSNs. We can now increase the network's capabilities in many areas, such as autonomous WSN deployment, flexible topology modification, and quick reaction to events, by bringing the notion of controlled mobility to WSNs. A complete review of current studies on WSN mobility is provided in this study proposal. There are four sections to this topic. We begin by looking at a few publications on the topic of network deployment helped by mobility. Second, we introduce mobile sensor-based functional enhancements. A hybrid WSN's sensor dispatch is the third topic on our list. Finally, we discuss the design of mobile platforms that facilitate sensor mobility and provide a variety of mobile WSN applications [4].

2 Problem

There has been a dramatic increase in wireless communication technologies that have fueled the development of sensor networks (WSNs). One or more distant sinks and several low-power sensor nodes equipped with actuators, sensors, and wireless transceivers make up a network like this. These nodes are widely dispersed around an area of interest in order to gather data from the area and send it back to central sinks on a regular basis. Wi-Fi sensor networks, on the other hand, may make it easier to keep tabs on real-world conditions. Object tracking, health monitoring, security surveillance, and intelligent transportation are just some of the WSN-related applications that have been developed in recent years. Typically, a WSN is installed with a fixed number of sensor nodes to monitor a certain area [5]. The following issues may arise if a static WSN is used in today's hostile environment due to the dynamic nature of events.

It is possible that the WSN's first deployment does not ensure full coverage of the sensing field and access to the network. Sensor nodes can be dispersed by robots or airplanes in difficult terrain. Even if we disperse a great number of nodes, we can't ensure that these randomly placed sensors will cover the whole region, and they may even be divided into numerous separate subnetworks that aren't linked to one another. Furthermore, the challenge might be made more complex by the shifting focus of research areas and the presence of roadblocks [6]. It is common for sensor nodes to be battery-powered and susceptible to failure. There may be gaps in the WSN's coverage if nodes die from running out of electricity. The network may also be disrupted by these dead nodes. It is difficult to recharge sensor nodes or deploy new nodes to replace the sensors that have died in many cases. Depending on the situation, the WSN may be called upon to assist with several tasks. Enough sensor nodes must be deployed along the target's path in order to effectively track an item; similarly, the perimeter of a boundary detection mission must have enough nodes to effectively monitor the target. Providing for every potential combination of mission needs would be prohibitively expensive, therefore deploying a large number of sensor nodes is not an option [7]. Some applications require pricey sensors to be used. It's conceivable, for example, that pressure sensors would be used in a military setting to keep an eye out for intruders. These sensors, on the other hand, can simply record information about what flows through them, not characterize it. The use of cameras or other high-tech sensing equipment is necessary for this instance. Despite this, the sheer number of nodes makes it impossible to install cameras on each one. We can improve a WSN's capabilities and flexibility to serve numerous missions and deal with the aforementioned issues by providing mobility to some or all of its nodes. Mobile WSNs and mobile ad hoc networks (MANETs) are fundamentally distinct from WSNs, which are typically thought of as ad hoc networks with sensing capabilities added on. There is no "deliberate" mobility in a MANET, but there is with a mobile WSN. To put it another way, we can use mobile sensors to carry out a variety of different tasks [8]. First, we'll look at several deployment strategies for rearranging a randomly deployed WSN into a more regular topology, which will allow the WSN to cover as much of the sensing field as possible [9]. A WSN's functionality may be improved by relocating mobile sensors, which we'll show you how to do in this section. This includes expanding the WSN's coverage area, connecting it to the network, and improving its detection capabilities.

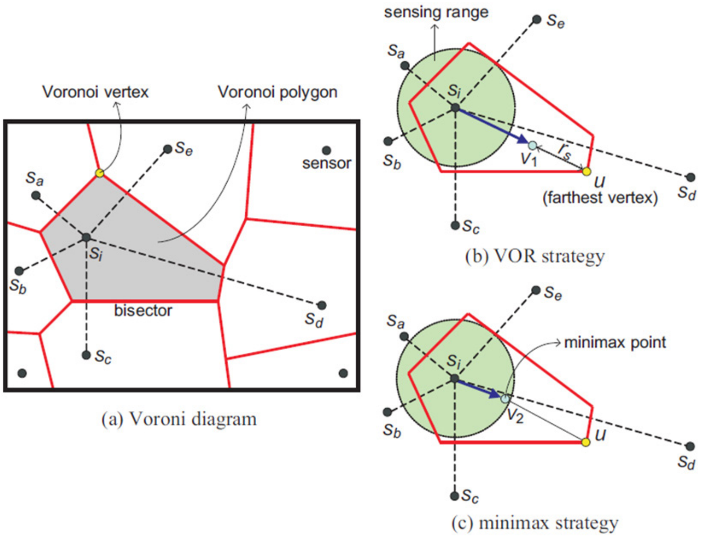
3 Goals

In WSNs, sensor deployment is critical since it directly impacts the network's detection capability. For the formation of a WSN, several studies have suggested various mobility-assisted deployment schemes They assume that a sensing field has a large number of randomly placed mobile sensors. In order to create a network of sensors that can cover the largest possible area, several movement tactics are employed [10].

The Force-Directed Deployment (FDD) method schemes assume that there are attractive and repulsive interactions between sensors and that these forces will cause sensors to move in response to these forces. The deployment of VORONOI-based systems Schemes employs a graph-based algorithm to predict coverage gaps and move sensors to fill them. Three. In the Deployment Planned Ahead of Time First, the sites for sensor placement are calculated, and then the sensors are efficiently dispatched to these areas.

4 Deployment methods based on the VORONOI

To identify possible coverage gaps, a Voronoi diagram is employed, and sensors are then moved to fill such gaps. Perpendicular bisectors of lines that link two nearby nodes produce the Voronoi diagram on a 2D plane, as seen in Figure. Using a Voronoi diagram, you may see the spatial closeness of a collection of geometric nodes [11]. This polygon's central node is closer than any other node to every point inside it. There may be a coverage hole within a Voronoi polygon if a sensor's detecting range isn't large enough to cover the entire polygon. To create the Voronoi polygon, all a sensor requires is the positions of its Voronoi neighbors. This means that each sensor can check for local coverage holes. A Voronoi polygon is formed by calculating each sensor's position in relation to its neighbors after the first deployment as in Figure 1. Then, three ways to relocate sensors are discussed:



(a) Voroni diagram

(b) VOR strategy

(c) minimax strategy

Fig. 1. Voronoi diagram based strategy

There are many uses for wireless sensor nodes, but they have one major drawback: their low power consumption. To address this issue, we need to improve the energy in wireless sensor networks without sacrificing their ability to gather information in diverse settings. Once a wireless sensor network is up and running, it may be impossible or unpleasant to do battery replacements on sensor nodes. Because of the energy constraints, designing long-lasting sensor networks is crucial and complex. To meet the sensor network's lifespan requirements, we investigate the deployment of sensor nodes. A design of this type has a wide range of potential freedoms [12].

5 Methodology, projected approach, and integrations

Sensor nodes are pushed by attracting and repulsive forces in force-directed deployment methods, so the sensor node moves in response to the communication needs of the network and its environment. ns2 will display it as a simulation. The Voronoi-based deployment techniques—To assess possible coverage between holes and shift sensors to cover these gaps accordingly. This method is to be used in a simulated environment [13]. Before deploying sensors, it's important to figure out the best places to position them in terms of energy efficiency. Simulator simulations are to be used to achieve this plan [14]. Sensors must be able to move and gather data in various settings, and these sensors must also be able to replace the failing sensor nodes and gaps between the nodes to collect information in an energy-efficient way through the suggested work. The results were compared to those from prior experiments [15–18].

5.1 Schemes for implementing

- The deployment strategies that are based on force.
- Secondly, the Voronoi-based deployment methods.
- Deployment plans that have been predetermined.
- Implementation of the proposed intelligent WSN system.

5.2 Key aim of the work

- To compare the outcomes with existing systems
- The relay nodes are used to link the wireless sensor nodes so that they can move freely, providing optimal efficiency.

Additionally, these sensors must be able to repair broken sensor nodes and gaps between nodes in order to collect information in an energy-efficient way. The results were compared to those from prior experiments. The goal of Wireless Sensor Networks is to reduce energy consumption and maximize usage while also prolonging the lifespan of the sensors involved. Sensing communication and connection are directly impacted by sensor location in wireless sensor networks. Before any data can be gathered, sensors must be installed. The battery capacity and the number of nodes around the environment restrict the sensor's lifespan. Because sensors can't be recharged during deployment, reducing power consumption and optimizing sensor lifespan are critical considerations. The nodes are permanently installed, and they collect data from their surroundings and transmit it to a distant sink. The primary purpose is to balance the competing goals of network coverage and energy usage in order to achieve the best of both worlds. Using microservers, the sensor's lifespan may be increased. Sensing and monitoring the network's relay are two of the sensor's most important functions. It's a huge undertaking to identify and monitor the important quantities, analyze and evaluate data and formulate useful display and decision-making information, as well as to conduct decision-making and alarm activities in the hierarchy. Distributed Wireless Sensor Networks, which are in charge of both sensing and processing at the earliest levels of the hierarchy, offer the data required for smart environments. The latest financing initiatives, notably the DARPA SENSIT program, military projects, and NSF Program Announcements, underline the relevance of sensor networks. To be successful in the field of wireless sensor networks, one must be well-versed in many other areas of study. Modern networks are bi-directional, allowing for sensor activity to be controlled as well. Many industrial and consumer applications, such as industrial process monitoring and control machine health monitoring, make use of wireless sensor networks, which were originally developed for military uses like battlefield surveillance. Constraints on power consumption for nodes utilizing batteries or energy harvesting are among the most important features of a WSN, as is the capacity to handle node failure, mobility, communication failures, heterogeneity of nodes, and the ability to survive harsh weather conditions.

5.3 A cross-layering approach

Wireless communication researchers are increasingly focusing on cross-layer communication. Traditional layering has three key drawbacks, as well. It's impossible to share information between layers in a traditional layered approach. This means that each layer does not have complete information. Network optimization cannot be guaranteed using the typical tiered technique. As environmental conditions change, the typical tiered strategy will be rendered ineffective. The standard tiered strategy for wired networks is not appropriate to wireless networks because of the interference between the different users, access conflict, fading, and the changing environment. It is therefore possible that the most efficient transmission performance measures, such as data rate and energy efficiency, can be improved by the application of cross-layer modulation [11]. A sensor node may be thought of as a little computer with the most rudimentary of interfaces. Processors and memory with limited computational power and memory, sensors or MEMS, a communication device (often radio transceivers or optical), and a power supply (typically batteries) make up the majority of these devices. Energy harvesting modules, supplementary ASICs, and a second communication interface are all possibilities. With larger computational, energy, and communication resources, base stations are one or more WSN components. Typically, they function as a gateway between sensor nodes and the end-user, passing data from the WSN to a server. Routers that are specifically built to compute, generate, and disseminate routing tables are another particular component in routing-based networks. A WSN system includes a gateway that connects wirelessly to the wired world and dispersed nodes [12].

1. Associated Resources
2. Possibilities for Use
3. WSN applications have been developed for a variety of industries, including health care, utility monitoring, and remote access. Wireless gadgets in health care provider for less intrusive patient monitoring and care. Wireless sensors may be used to acquire system health data at a reduced cost for utilities such as the power grid, streetlights, and water municipalities. Wireless systems can complement wired systems

by decreasing cable costs and enabling new forms of measurement applications in remote monitoring, which covers a wide variety of applications. Applications for remote monitoring include air, water, and soil monitoring; building and bridge structural monitoring; machine monitoring in the industry; process monitoring; and asset tagging.

4. Read the case study to see how researchers are monitoring carbon transport in rain forests using wireless instruments. NI Lab VIEW and Compact RIO are used by researchers to monitor the environment in the Costa Rican rain forest.

Some people benefit from wireless technology because they know how to use both wired and wireless systems in their applications [8]. The NI LabVIEW graphical system design platform can help you achieve this goal. A broad variety of wired and wireless devices may be connected with Lab VIEW. There are three common topologies for WSN nodes: ring, mesh, and star. Each node is connected directly to a gateway in a star architecture. Network data is directed from the node closest in the cluster hierarchy upwards until it reaches a gateway, which links all nodes to each other and a higher node. Finally, mesh networks have nodes that may connect to numerous nodes in the system and transfer data through the most reliable way available to provide greater dependability. A router is a common term for this type of mesh connection.

5.4 Power optimization aspects

For example, sensors dropped from aeroplanes for personnel/vehicle surveillance are being used in ad hoc networks of geographically spread sensors at remote site contexts (e.g. power production, power conservation, and power management). Transceivers' capacitors, inductors, and other microelectromechanical systems (MEMS) components are the focus of current research. The fabrication of micro-sized inductors has become the bottleneck. Solar vibration (electromagnetic and electrostatic), thermal, and other technologies are being used to build MEMS power producers. Microcircuits with an L-C tank circuit that saves power from received interrogation signals and then transmits a response are known as RF-ID (RF identification) devices. In contrast to passive tags, which have no power source or storage capacity, active tags are equipped with a battery and can store up to 1Mb of data. In the low-frequency range of 100 kHz–1.5 MHz or the high-frequency range of 900 MHz–2.4 GHz, the operational range of radio frequency identification systems is up to 30 meters (100 feet). There are several uses for RF-ID tags, including inventory control in manufacturing and sales, container tracking, and more. A metering truck may drive by and read the current readings of water meters that have RF-ID tags affixed. They can also be found in vehicles to collect tolls automatically. Software power management approaches, on the other hand, may significantly reduce the power used by RF sensors. For power conservation purposes, the node can be powered down or "sleep" between its allocated periods, waking up in time to receive/transmit messages [9].

5.5 The architecture diagram

In our approach, if a sensor node attempts to send a packet to another sensor node in order to execute an action, it uses the most efficient method. Sensor nodes now have GPS built-in, making it easier to follow them than it was in the days of the old approaches. Header node and base station transmit location-specific information to the server. Energy efficiency is maintained by lowering bandwidth utilization, such that by eliminating the search for other nodes for communication, which causes the waste of energy in the sensor node, our solution considerably decreased it. Sensor nodes are organized into groups in this suggested technique, and each group should have a head sensor node.

- The base station receives information about other nodes from the head sensor node.

Additionally, this data is transmitted to a server or central monitoring system by the base station itself.

6 Results and snapshots on simulation attempts

Existing systems

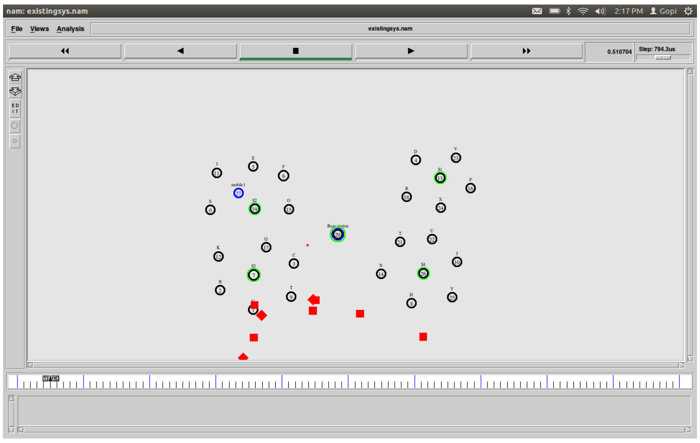


Fig. 2. Nodes scenario in simulation

Figure 2 depicts the ns2 environment with nodes deployment so that the implementation scenario can be simulated.

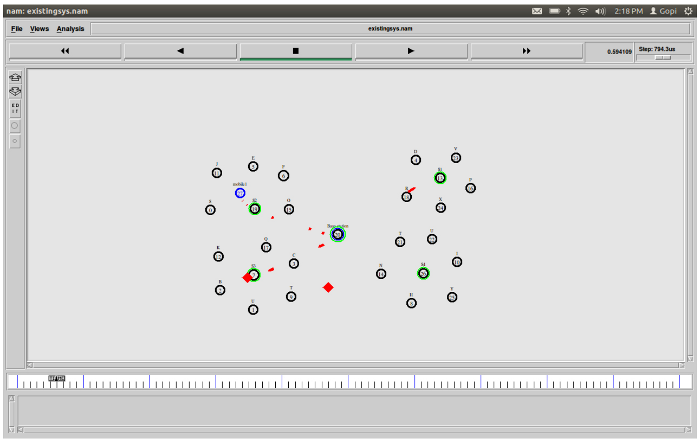


Fig. 3. Mobile nodes connection with base station

Figure 3 depicts of connection aspects of the node with the base station so that connectivity is analyzed.

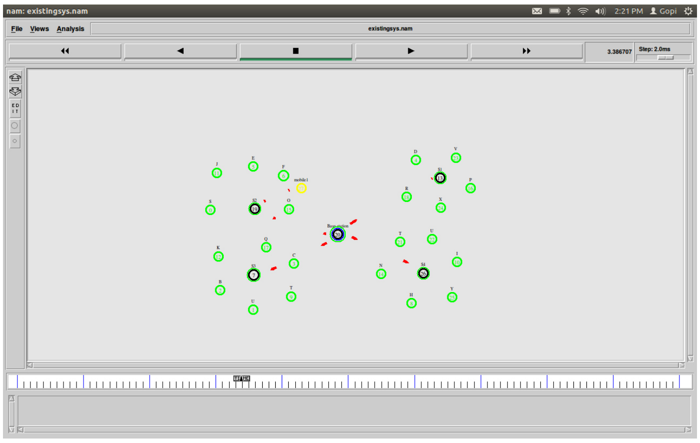


Fig. 4. Mobile nodes in the movement and communication tracks

Figure 4 analyze the track of mobile nodes in wireless environment so that any attack can be tracked.

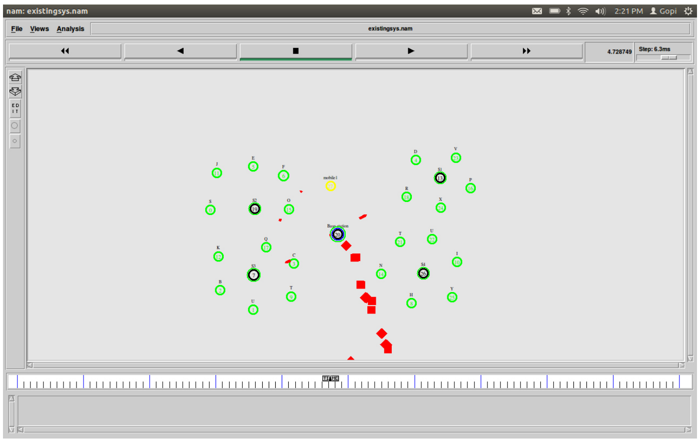


Fig. 5. Tracking of nodes

Figure 5 presents the scenario of packet drop on the attempt of attack and is tracked in the simulation. Proposed System with Projected Simulation

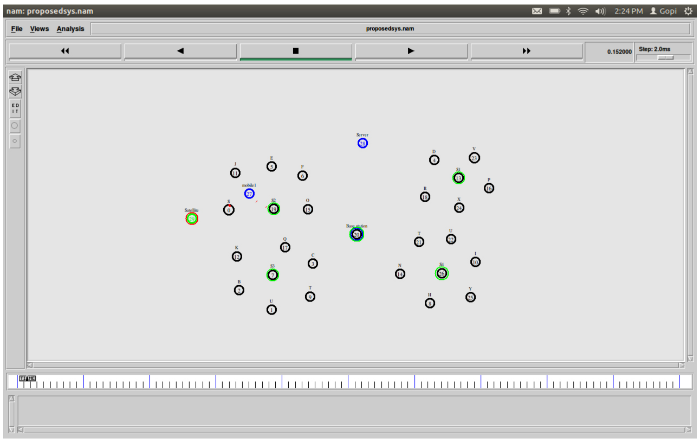


Fig. 6. Movement and positional points

Figure 6 presents the positions of each node with the security aspect and real time tracking.

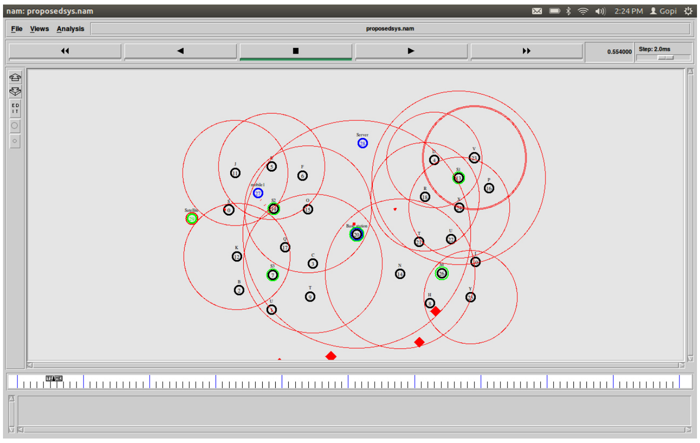


Fig. 7. Acknowledgment with base station

6.1 Comparison graph

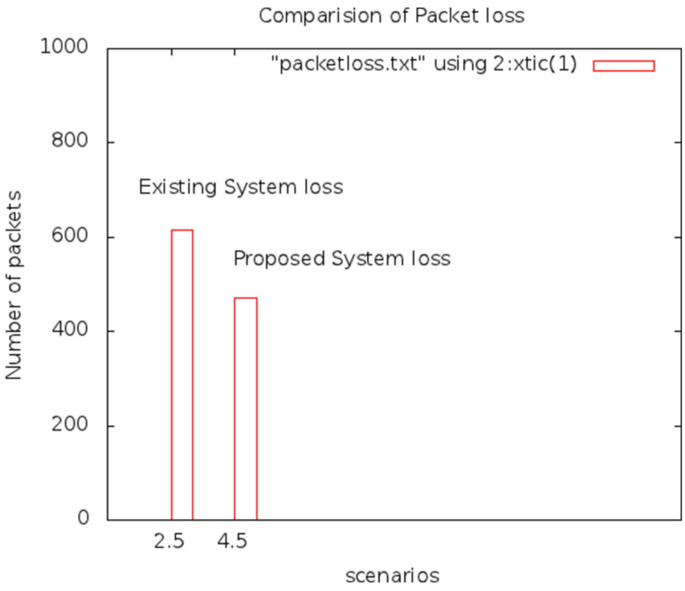


Fig. 8. Packet loss analytics

Security and integrity are compromised by the current system's use of the classical method. In order to prevent attacks from occurring through any channel, the strategy must be modified.

- The current system is inefficient with regards to packet loss, jitter, and throughput.
- Sybil attacks on network infrastructure should be avoided using a particular mechanism and algorithmic technique. The Sybil attack is a particularly damaging assault that exploits these properties, in which the hostile node fraudulently claims many identities. As a result of a Sybil assault, a wide range of network functions, including data aggregation, voting, and resource allocation, can be severely disrupted. The algorithmic strategy for the mechanism against Sybil assaults must be developed and simulated specifically.

6.2 Key advantages of proposed system

Network nodes requesting services like the internet register their identities with a server agent, which returns a unique ID to the asking node. When a source node requests a route to a destination node via the current access point, the current access point transmits the route request to the server agent. It checks source ID, approves route requests from the sender, and then gets receiver information using destination ID from a list of available destinations. Following this broadcast, the server agent notifies the registered neighboring nodes that are closer to the destination and ready to offer service of the route request, and the server agent receives an acknowledgment message. A nearby node with a long life duration (the ability of nodes to stay linked to the destination node) is selected by server agents based on the ID data, which also includes information about a node's position, the direction of movement, and speed. Afterward, the server agent sends the source node a route reply message, and the source node begins securely transferring data packets.

- The server agent promptly replaces any nodes that leave the network with others in order to preserve the continuity of the connection. A server agent takes full control of the ad-hoc network in this method, eliminating any malevolent or selfish nodes from the network. In terms of finding the best possible answer, the suggested method performs well when used in conjunction with a technique to prevent Sybil attacks.
- Despite a large number of repetitions, the suggested method has low Jitter and high throughput. It's possible that the presented work has certain limits in terms of how it might be improved utilizing various parallel algorithmic techniques. Simulated annealing, a popular genetic algorithmic approach, may improve the suggested system's performance.

7 Conclusion

Wireless Networks and Ad-hoc network security concerns will be addressed, as well as the advantages and disadvantages of mobile network protocols, in this study. The security of MANETs has been the subject of several studies, but none of the protocols has emerged as the best in terms of both security and performance. There are several flaws in the Mobile framework, which might lead to random connections from unknown nodes without the correct routing is in place. We're going to focus on making the Mobile Ad-hoc network more secure in order to keep other nodes from invading. Security was one of several important concerns among many others in a wide range of study topics. It's been difficult for a long time to secure this open network because of the lack of suitable infrastructure. Traditional network security methods are no longer viable in today's technologically advanced society. Many levels are susceptible to man-in-the-middle assaults or multilayer attacks, thus proposals should focus on these layers. Security for the network has not yet been achieved using an intelligent technique. Ad-hoc Networks rely on any fixed infrastructure or any other mobile node to interact via packet forwarding and reception. There is no proper infrastructure for forwarding and receiving packets in a wireless ad-hoc network compared to a wired ad-hoc network, allowing both authorized users and hackers to access it. In this wireless ad-hoc network, there is no design to monitor traffic and accessibility, which leads to a third-party intervention like malicious users. Applications A better knowledge of QoS parameters may be achieved and they can be utilized to solve different networking challenges. It gives a comparative analysis on systems under the parameters packet loss, packet delivery rate, and network connectivity.

8 References

[1] Nazir, R., Kumar, K., David, S., & Ali, M. (2021). Survey on wireless network security. Archives of Computational Methods in Engineering, 1–20. https://doi.org/10.1007/s11831-021-09631-5

[2] Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A review of ip and mac address filtering in wireless network security. Int. J. Sci. Res. Sci. Technol, 3(6), 470–473.

[3] Jiang, F., & Tseng, H. W. (2019). Trust model for wireless network security based on the edge computing. Microsystem Technologies, 1–6.

[4] Didmanidze, I., Beridze, Z., & Zaslavski, V. (2020, October). Analysis of wireless network security systems problems and those solutions. In Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference (No. 4, pp. 139–140). https://doi.org/10.31713/MCIT.2020.31

[5] Lin, Y., Li, W., Sun, J., & Wu, Q. (2018, April). Improving wireless devices identification using gray relationship classifier to enhance wireless network security. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 421–425). IEEE. https://doi.org/10.1109/INFCOMW.2018.8406960

[6] Sagduyu, Y. E., Shi, Y., & Erpek, T. (2019, June). IoT network security from the perspective of adversarial deep learning. In 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 1–9). IEEE. https://doi.org/10.1109/SAHCN.2019.8824956

[7] Kostadinov, G., & Atanasova, T. (2019). Security policies for wireless and network infrastructure. Problems of Engineering Cybernetics and Robotics, 71, 14–19.

[8] Jiang, R., & Zhang, X. (2020). Application of wireless network control to course-keeping for ships. IEEE Access, 8, 31674–31683. https://doi.org/10.1109/ACCESS.2020.2973464

[9] Fikriyadi, F., Ritzkal, R., & Prakosa, B. A. (2020). Security analysis of Wireless Local Area Network (WLAN) network with the penetration testing method. Jurnal Mantik, 4(3), 1658–1662.

[10] Ghosh, T. C., & Jabiullah, M. I. (2021). Analysis of network security issues and threats analysis on 5G wireless networks. Recent Trends in Information Technology and its Application, 4(3).

[11] Rath, M., Swain, J., Pati, B., & Pattanayak, B. K. (2018). Network security: Attacks and control in MANET. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 19–37). IGI Global. https://doi.org/10.4018/978-1-5225-4100-4.ch002

[12] Wu, H. T., & Horng, G. J. (2017). Establishing an intelligent transportation system with a network security mechanism in an Internet of vehicle environment. IEEE Access, 5, 19239–19247. https://doi.org/10.1109/ACCESS.2017.2752420

[13] Ibraim, D., & Zebur, B. (2020). Main tasks and algorithms of wireless network security supporting automated system. Problems of Atomic Science and Technology, Series: Nuclear Physics Investigations (74), (5), 129.

[14] Geetha, R., Suntheya, A. K., & Srikanth, G. U. (2020). Cloud integrated IoT enabled sensor network security: Research issues and solutions. Wireless Personal Communications, 113(2), 747–771. https://doi.org/10.1007/s11277-020-07251-z

[15] Alaidi, A. H., Soong Der, C. S., & Weng Leong, Y. (2021). Systematic review of enhancement of artificial bee colony algorithm using ant colony pheromone. International Journal of Interactive Mobile Technologies,15(16), 173. https://doi.org/10.3991/ijim.v15i16.24171

[16] Alrikabi, H. T., & Tuama Hazim, H. (2021). Enhanced data security of communication system using combined encryption and steganography. International Journal of Interactive Mobile Technologies, 15(16), 144–157. https://doi.org/10.3991/ijim.v15i16.24557

[17] Nabaa Ali Jasim, H. T. S. A. (2021). Design and Implementation of smart city applications based on the internet of things. International Journal of Interactive Mobile Technologies (iJIM), 15(13), 4–15. https://doi.org/10.3991/ijim.v15i13.22331

[18] Zhang, D., & Liao, S. Y. (2020, November). The security based on wireless network in nuclear power plant. In Internationael Symposium on Software Reliability, Industrial Safety, Cyber Securityse and Physical Protection for Nuclear Power Plant (pp. 64–70). Springer, Singapore. https://doi.org/10.1007/978-981-16-3456-7_8

9 Author

Prof. Dr. Sundresan Perumal in College of Information Technology, Islamic Science University, Malaysia (sundresan_197@gmail.com).

Article submitted 2022-02-14. Resubmitted 2022-03-11. Final acceptance 2022-03-11. Final version published as submitted by the authors.