An Escalated Performance Aware Approach for Cumulative Effectiveness in Mobile Ad-Hoc Networks

https://doi.org/10.3991/ijim.v16i10.30041

Karl Brown(✉)
College of Computer Sciences, Texas Tech University, Texas, USA
karlbrown@yahoo.com

Abstract—In order to provide secure communication between mobile nodes in a hostile environment, security has become a top priority. There are a variety of nontrivial difficulties to security design in mobile ad hoc networks because of its unique properties, such as open peer to peer network architecture and shared wireless medium. Building multi-layered security systems that provide broad coverage while still delivering optimal network performance makes perfect sense in light of these problems. Specifically, in this study, we address the basic issue of maintaining the multi-hop network connectivity between mobile nodes in a Mobile Ad Hoc Networks (MANET). There are a number of security concerns that need to be addressed in order to safeguard the multihop wireless channel's MANET connection and network layer activities when delivering packets. We go through these difficulties and possible solutions in this paper. Complete security solutions should cover both layers and include the prevention, detection and response aspects of the three components of the security system. Providing secure communication between mobile nodes in a hostile environment has become a top priority. For example, the open peer-to-peer architecture, shared wireless medium, resource limits, and high dynamic network topology of mobile ad hoc networks provide a variety of nontrivial security design difficulties. The work integrates the effectual approach with the integrity and performance aware implementation for the Mobile Adhoc Networks.

Keywords—mobile Ad Hoc networks, MANET effectiveness, performance in MANET

1 Introduction

Without the need for a physical infrastructure or hardware environment, wireless communication including MANET allows packets and network signals from source to destination to be sent securely and privately [1, 2].

As a result, the entire communication may be maintained for an extended period of time with a better degree of performance and accuracy level thanks to a variety of wireless channels [3–7].

The following items are often found in a wireless system:

System components include: a base station, radio frequency modules, sensor nodes, mobile nodes, satellite components, a tower, and radio signals. Deep investigation systems include: receivers, transponders, and transmitters, as well as a controller and mobile nodes [8–11].

This scenario is constructed by using these items to broadcast and receive signals so that the specific purpose may be realised in the wireless environment.

Table 1. Comparison aspects of wireless networks technology

	Bluetooth	**WiFi (a)**	**WiFi (b)**	**WiMAX**	**WiFi (g)**
Limitations	Range Issues	Cost Factor	Speed	Cost	Cost and Range both
Range Parameter (meters)	10	50	100	50	100
Frequency (In GHz)	2.45	5	2.4	2–66	2.4
Range Parameter (meters)	10	50	100	50	100
International Standard	802.15	802.11a	802.11b	802.16	802.11g
Range Parameter (meters)	10	50	100	50	100
Range Parameter (meters)	10	50	100	50	100
Advantages	Low Cost	Speed	Low Cost	Speed, Range	Speed
Range Parameter (meters)	10	50	100	50	100
Speed (In Mbps)	0.72	54	11	80	54

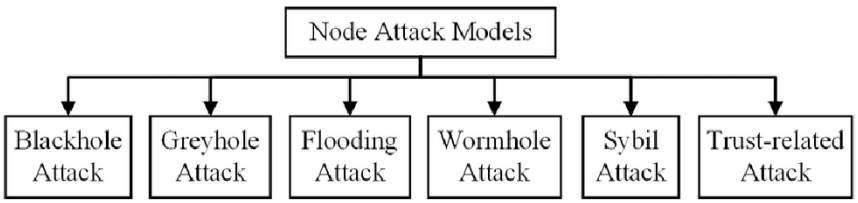


Fig. 1. Attacks on wireless networks

Table 2. Top countries affected by the malware attacks in terms of users

Countries	**Number of Users Attacked**
Brazil	91891
Russia	85817
US	66687
Germany	51661
UK	25256
India	22072
Turkey	21385
Australia	18692
Italy	17762
Spain	17614

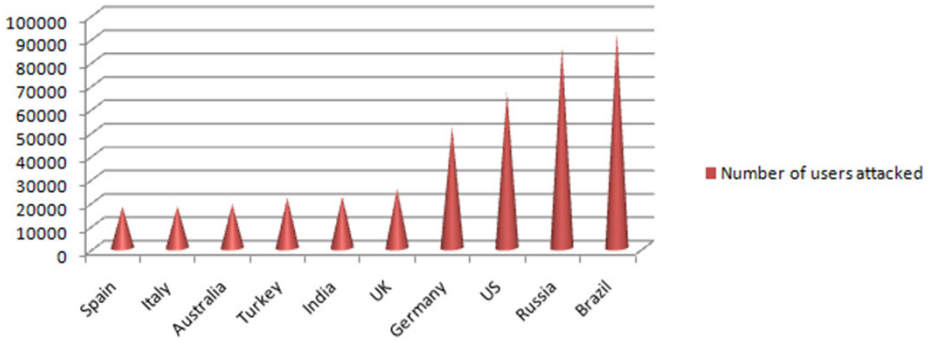


Fig. 2. User attacks on wireless

While the cluster head processes data packets and signals, the source is responsible for initiating transmission. After the data and signals from the source nodes have been aggregated, the base station or tower is utilised to maintain regular connection with the cluster head. There may be a number of sources of communication in the network. In local communication, the cluster head keeps track of all of the information exchanged between the nodes in its vicinity [12–16].

Nearby nodes or related nodes have access to a group head or cluster head so that they may directly interact with the local node without depleting the energy of the satellite or direct controllers, which is a frequently used paradigm in wireless sensor networks [17–21].

Here are the aspects and dimensions that determine which node will be designated as the network's cluster head: Lifetime Fitness Value; Appropriate Channel; Speed; Threshold Aspects; Security; Integrity; Threshold Evaluation; Transparency without Bias; and Energy Value; Cavernous Penetration; Deep Penetration; Maximum Connections; and Cavernous Key Points [22–26].

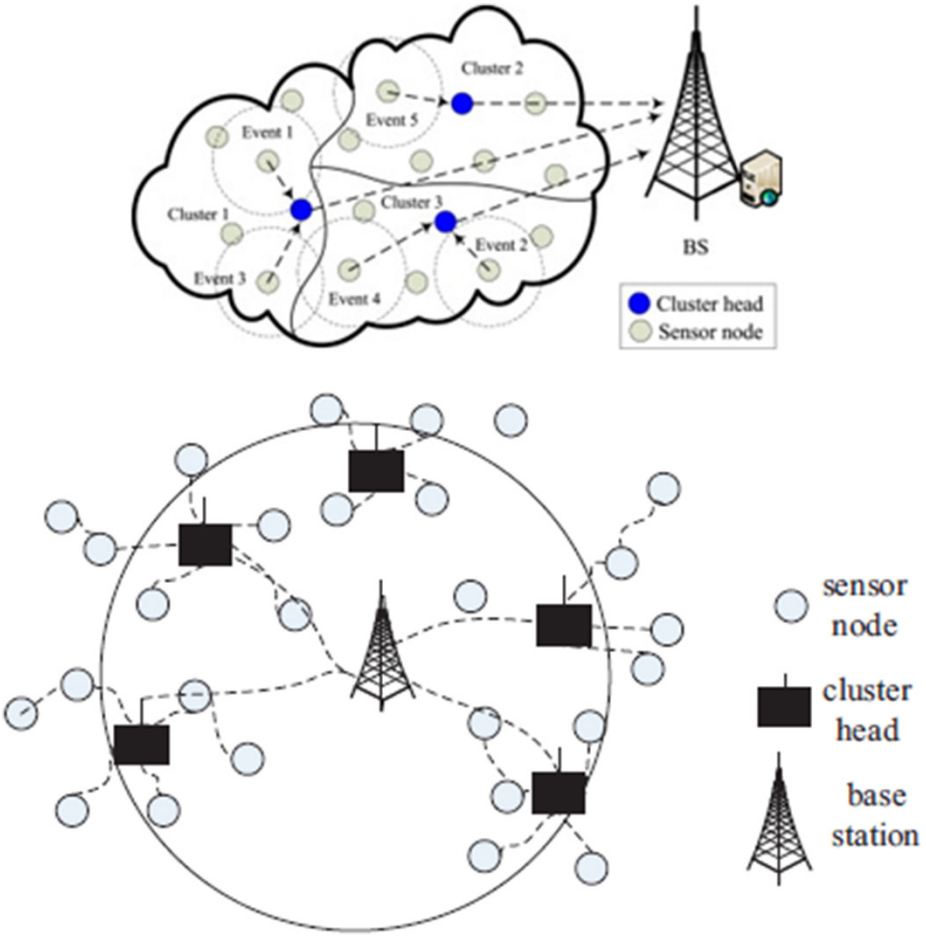


Fig. 3. Secured cluster head with different events

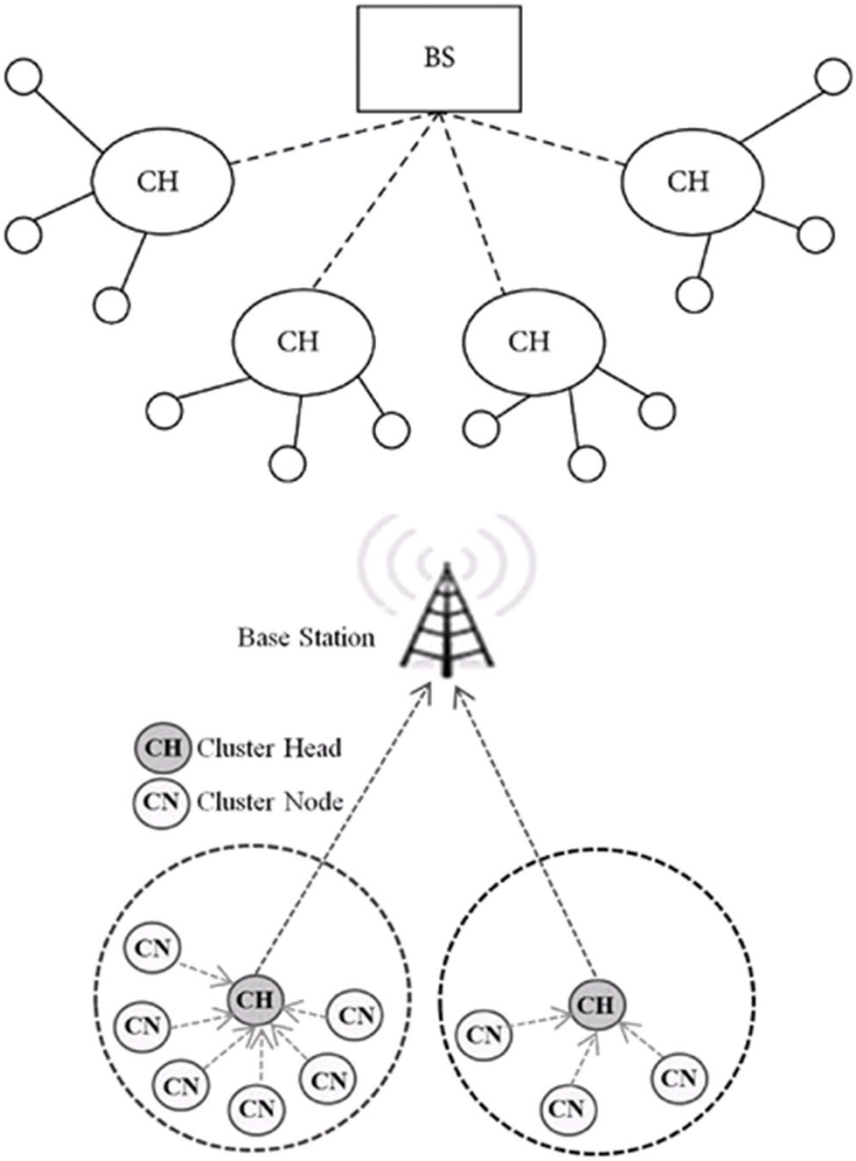


Fig. 4. Base station and clusters

A wireless network depicted in the figure shows the cluster head and its associated cluster node communicating with the base station so that total transmission may be accomplished [27].

2 Problem

A number of Vulnerabilities and Risks are associated with Wireless Environment. A snooping assault is one in which eavesdropping or intercepting communications is

carried out in the shadows. This sort of attack on wireless security involves an aggressive examination of network channels.

Using virtual work to intercept the network's communications, a base attack is carried out. A convoluted assault is one in which the network is given the Convolutional path or complicated path for the goal of doing harm. It's used to get data packets without authorization from network nodes and abuse them [27].

Assault speeding up the attack means that more energy can be used in an immoral manner. The enticing elements of the non-authenticated nodes in the network environment might have a significant impact on the network's security.

This form of assault chokes down the network channel and bandwidth, causing the bandwidth to be depleted to a large extent. To interrupt and harm communication among the real and authenticated network users, this method consumes and substantially loads network bandwidth.

When it comes to security, the Data Encryption Standard (DES) refers to a strategy that ensures that data is encrypted to the highest possible level of security in order to ensure that the whole connection is cryptographically secure and trust based [28].

Goals

- MANET Security: Improving Effectiveness and Elevation
- Wireless Scenarios with a Secured Approach
- The Use of Soft Computing for Wireless Network Security
- Formation for a Safe Approach
- Cyber-security on the MANET using soft computing
- Energy-based method to node preservation
- Security-Aware Networks for numerous nodes and testing on multiple simulators
- Analyzing and Assessing the Results Based on a Variety of Parameters

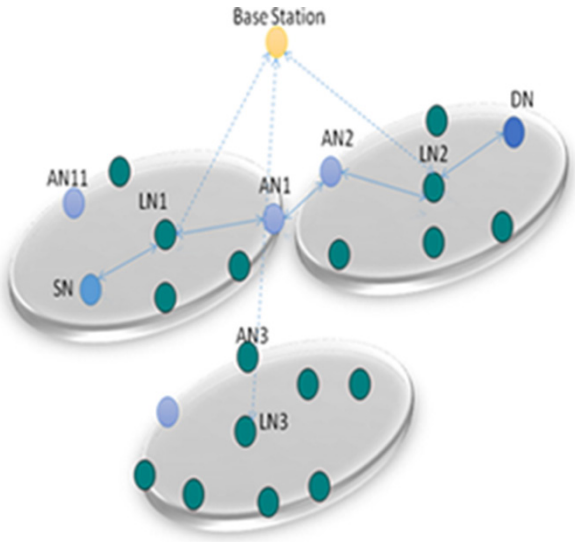


Fig. 5. Proposed integration

3 Methodology and architectural approach

In order to protect the network infrastructure against numerous anonymous assaults, network administrators utilise a variety of methodologies and strategies. Packet capture is one of the most common and well-known tasks that network administrators conduct.

Using this method, packets moving via the network may be fetched, and any suspicious activity can be discovered. Finally, the intrusion detection system (IDS) tools classify assaults or traffic types based on any out-of-the-ordinary or aberrant activities. The PCAP (Packet Capture) Files retrieved from honeypots or servers can be classified using a wide range of IDS tools, many of which are free and open source [29].

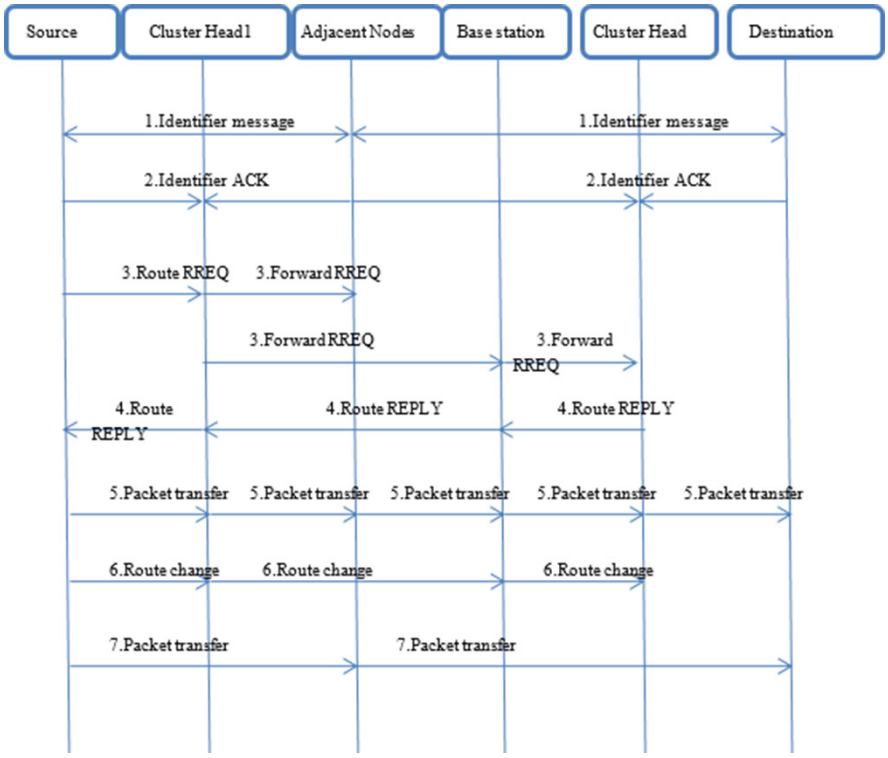
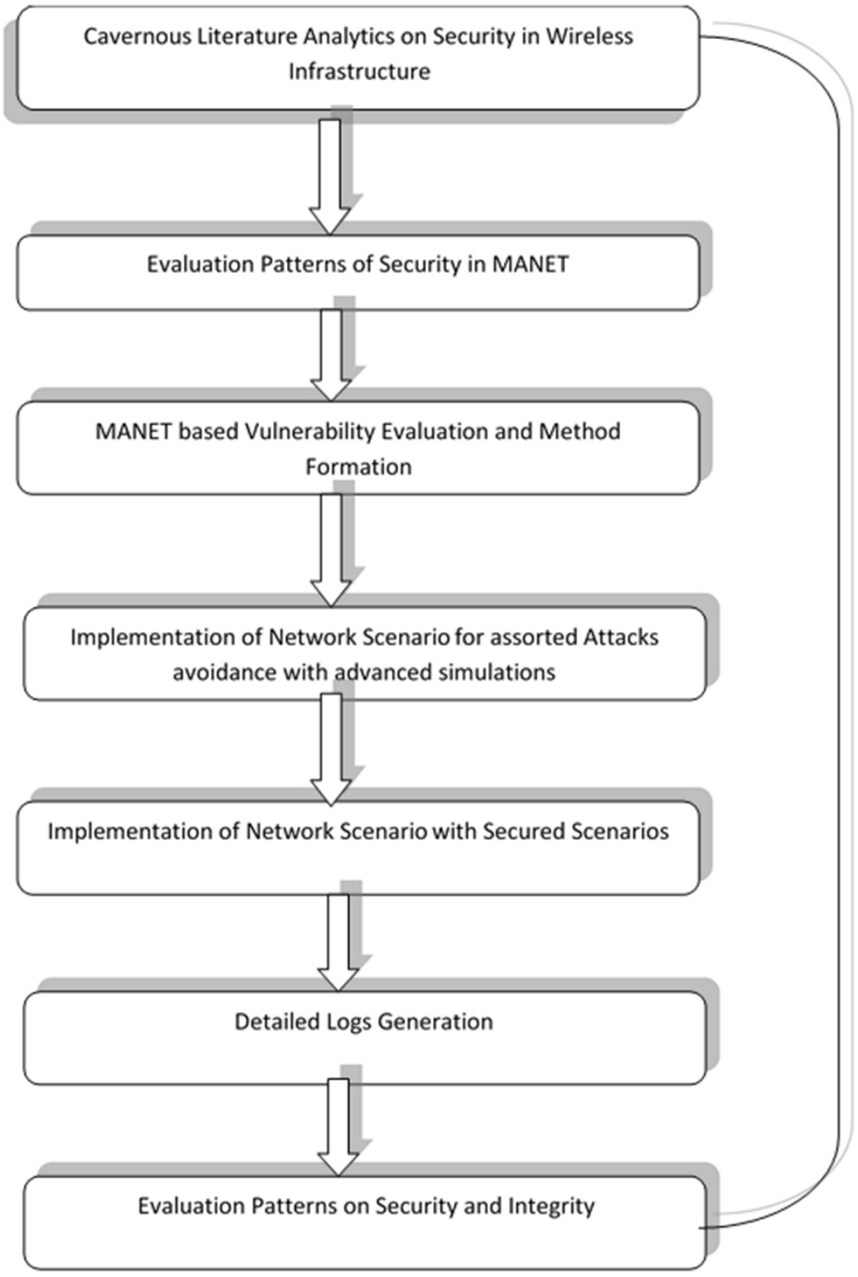


Fig. 6. Phases and transformation

Data on the number of malware assaults by country has been included in the analytics. These virus assaults have a global impact, as can be shown by the diverse locations they have infected. The data in this table depicts the total number of people who have been subjected to massive attacks and vulnerabilities in various nations throughout the world. There are a wide range of malicious behaviours that may be carried out by malware, such as the destruction of a system, the acquisition of monetary gain, the expansion of unauthorised access to the system, the disclosure of basic data, and so on. Malwares are designed to carry out a variety of dangerous actions, such as destroying a system, gaining monetary gain, increasing unauthorised access to the system, causing

security corruption, or spilling basic information or performing refusal of administration attacks [30–33]. A variety of sources, both intentional and unintentional, can introduce this infection onto the system. It's important to examine malware evasion techniques while setting up remote communication conditions to ensure security and honesty are not compromised, and to have a greater degree or trust in the particular system condition for individual or corporate use.

Analysis of the results of the simulation.



4 Results

Implementation Tool and Programming Platform: Network Simulator ns2
Operating System: Ubuntu Linux

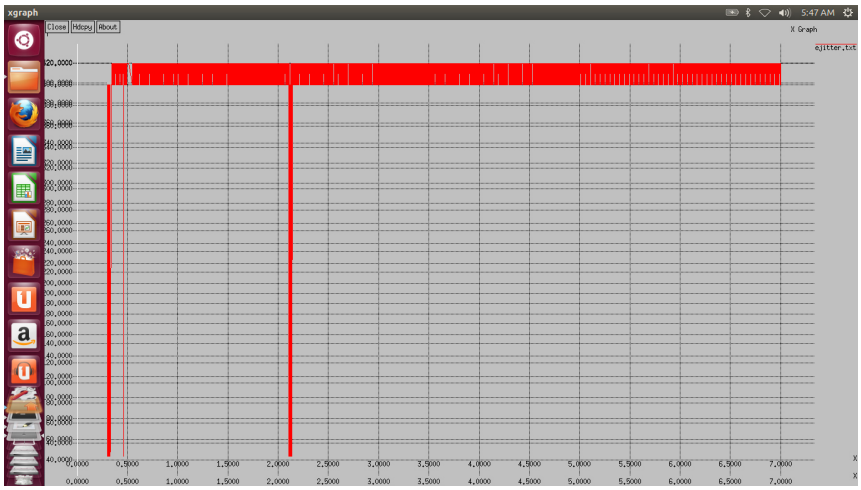


Fig. 7. Jitter evaluation patterns

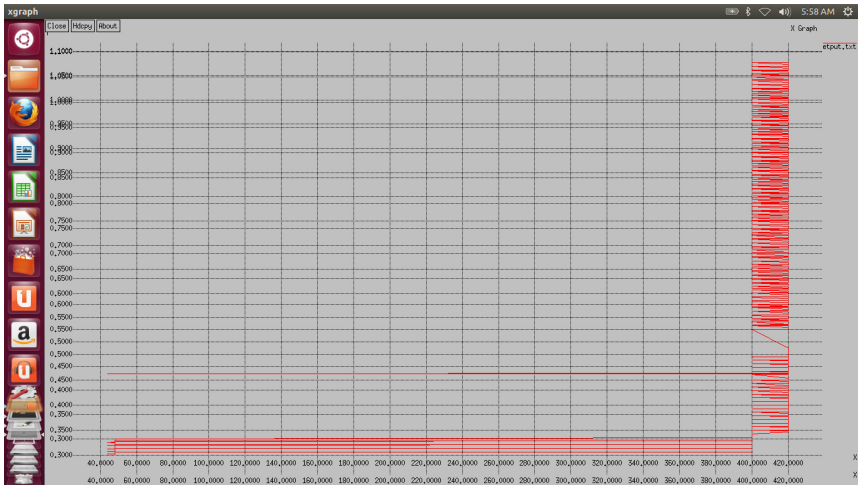


Fig. 8. Throughput evaluation patterns

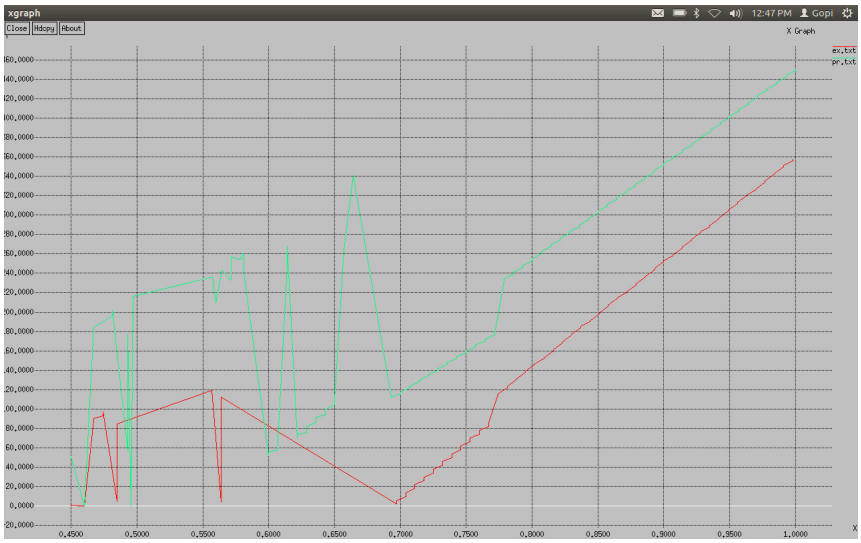


Fig. 9. Data transfer analytics evaluation patterns

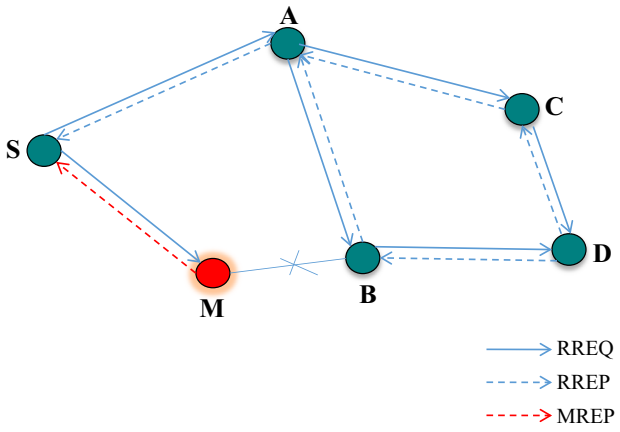


Fig. 10. Black hole attack

Static Integration Approach for Static Security Key Transmitted %*(!&^%*&*$^)(*

Static Integration Approach for Static Security Key Transmitted from simulation Broker . trcmpogcuan4¤??¦¨«ª?¥--

Randomly Selected Number of Processors int in a range : 29

Simulation Implementation pattern Time Evaluation in MillSeconds . 228

Novel Security Integrated Approach and Parameter . 20.47202020627282

06-20 22 : 55 : 22.222

Static Integration Approach for Static Security Key Transmitted .

%*(!&^%*&*$^)(*
Bandwidth . 2000
Processors . 9
and
VM Manager . Xen
Initialized
Security Key Not Matched... Operation Terminated
Simulation Implementation pattern Finish with NON-MATCHING (AUTHENTICATION FAILED) of the Keys
Operation Terminated
Simulation Implementation pattern Time Evaluation in MillSeconds . 229
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
2
Real Time Generation of Key
656
Security Integrated Architecture Integrated Key
656
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Success
success =
2
Failure =
4
Security Factor =
2 2 2 2 2 2
Security_Aware_Approach Integration Score =
82 82 82
Classical Static Greedy Integration Approach with Scoring Factor =
22 22 22
Real Time Generation of Key
727
Index =
727 22 277 47 98
MANET_Sec_Key =
5
Real Time Generation of Key
727
Security Integrated Architecture Integrated Key
98
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
4

Real Time Generation of Key
727
Security Integrated Architecture Integrated Key
47
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
2
Real Time Generation of Key
727
Security Integrated Architecture Integrated Key
22
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
5
Real Time Generation of Key
727
Security Integrated Architecture Integrated Key
98
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
2
Real Time Generation of Key
727
Security Integrated Architecture Integrated Key
727
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Success
success =
2
failure =
4
Security Factor =
2 2 2 2 2 2
Security_Aware_Approach Integration Score =
82 82 82 82
Classical Static Greedy Integration Approach with Scoring Factor =
22 22 22 22
Real Time Generation of Key
429
Index =
429 282 766 796 287
MANET_Sec_Key =
2

Real Time Generation of Key
429
Security Integrated Architecture Integrated Key
766
Response Generated by the Network =
Malicious Traffic Node Security Vector with Energy Transmission Failed
MANET_Sec_Key =
2
Real Time Generation of Key
429
Security Integrated Architecture Integrated Key
766
Response Generated by the Network =
Scenario67 Index67 Node67 7 Vector67 ELHO67 Module67 MANET-MessageBroadcast67
49.56474475 942225 247272 972292 226278 458285 955928 429485 262848
Scenario68 Index68 Node68 8 Vector68 ELHO68 Module68 MANET-MessageBroadcast68
67.48822222 246922 422242 694628 854246 659996 924542 656222 285775
Scenario68 Index68 Node68 8 Vector68 ELHO68 Module68 MANET-MessageBroadcast68
224.2774825 698425 824222 268242 872454 998765 252262 272828 226626
Scenario69 Index69 Node69 9 Vector69 ELHO69 Module69 MANET-MessageBroadcast69
29.45222726 227728 878248 528672 948826 682227 225578 527272 779489
Scenario69 Index69 Node69 9 Vector69 ELHO69 Module69 MANET-MessageBroadcast69
79.26662248 989224 284752 899662 896822 478429 622288 725522 289422
Scenario72 Index72 Node72 2 Vector72 ELHO72 Module72 MANET-MessageBroadcast72
52.46572592 282272 988254 892249 574782 627698 478462 252222 477855

Researchers characterizes look into worldview is the plan and the treatment of the examination by the agent in building up the investigation results. Research is trans-disciplinary in nature. Research worldview is the standard methodology by the examiner and it takes after the logical strategy for activity in procuring the outcomes. Research in every case coordinate towards the discovering answers for the issue surrounded and builds up the hypothesis and standards. Research worldview is the principal endeavor by the agent and the individual picks the strategy for taking care of the total examination from the two primary classifications as positivism and Interpretivism.

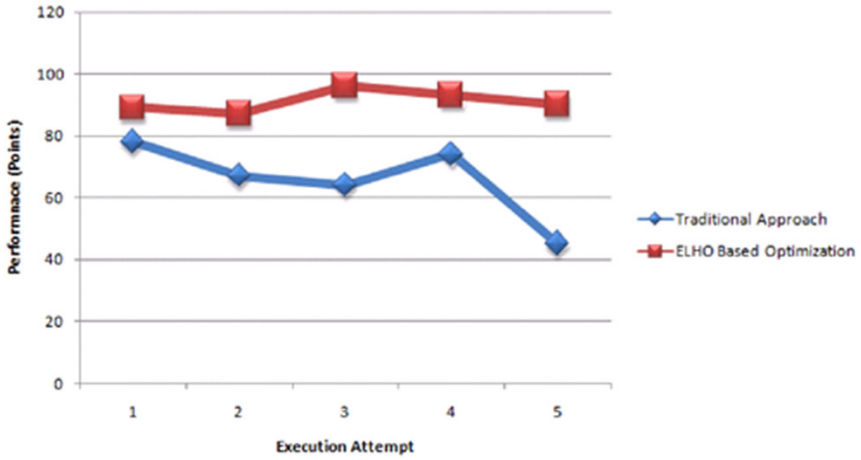


Fig. 11. Evaluation of performance

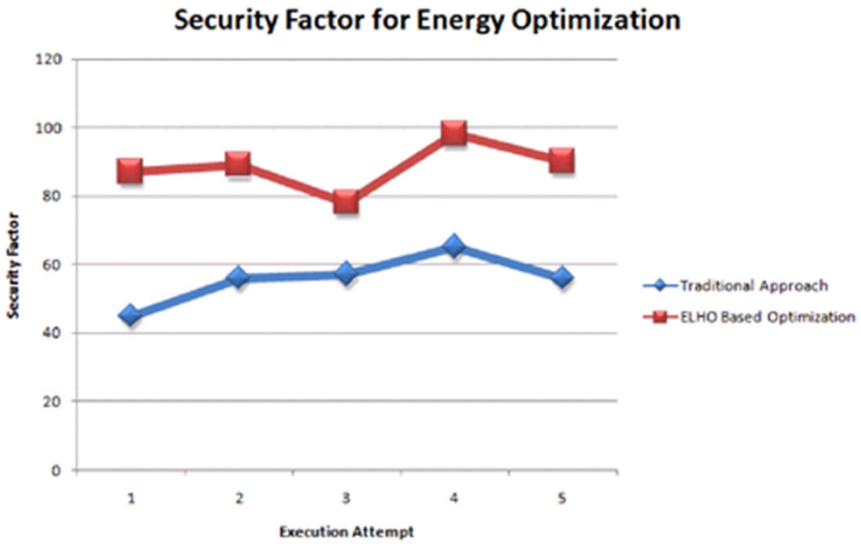


Fig. 12. Evaluation of security

5 Matrix based evaluation

The following output extract is fetched from the MATLAB Simulation with Biograph Toolbox integration. In the proposed work, we have generated a dynamic matrix of the base stations and wireless sensor nodes. The minimum distance vector is measured from the base station with the sensor nodes willing to communicate with the other node or station. By this way in the proposed approach, the lifetime of sensor

nodes are improved by the fact that the dying time or dying cycle of the sensor nodes are increased.

Using this approach of nearest and best fit base station, the energy level of the sensor nodes are maintained and improved. By increasing the energy level of the sensor nodes, the lifetime of sensor network and overall efficiency is improved. The simulation approach is making use of the Euclidean Distance Measurement is implemented for finding out the distance between base stations and wireless sensor nodes.

The initial energy levels of the network nodes are taken random in nature so that the effective and unbiased results can be obtained.

```
bs2
    5    9
Distance Aspect from Base Station
    2.2229
Tower
    7    6
Distance Aspect from Base Station
Distance Formulation =
    5.6569
Aspect
d =
    2.227229    2.229229    5.226569
Minima
    2.2229
Mean
    3.7722
n2 =
    3    2
Rounds
    2.2750e+03
Security and Performance Aspect
    -2.0629e+06
Routing
    2
Distance Aspect from Base Station
n2 =
    3    2
Monitoring
    2    0
Distance Formulation =
    2.2229
bs2
    5    9
Routing
    2
Distance Aspect from Base Station
```

6 Conclusion

In this study, several simulation scenarios are used to address various optimization elements, including energy optimization. In the field of energy optimization, there is still much to learn. Hyper-heuristics can be used for deep learning and predictive analysis of energy optimization and optimization. Nearly all metaheuristic implementations search in the search space in terms of issue solution spans, which is the primary demarcation line between metaheuristics and hyperheuristics. When it comes to hyper-heuristics, cases and search space are taken into account within the heuristics' scope. Interconnectivity is increasing at a rapid rate in the contemporary digital world and globalisation period. Our modern world is filled with a variety of technologies, such as smart phones and wifi nodes, that are always linked to the internet. The Internet of Things (IoT) is a popular area of wireless networking that makes it possible to connect physical items in the real world. Using IoT, actual items in the real world may interact and share information with each other in real time, with a greater degree of performance and security, thanks to their ability to connect. Smart items that can be controlled remotely are the focus of the Internet of Things (IoT). The findings show that the predicted strategy has the largest block size with the fewest rounds and is successful in collisions. It is possible to use this strategy in various IoT protocols and implementations for key generations that are performance sensitive in terms of energy optimization and may therefore be accepted.

7 Acknowledgment

You may mention here granted financial support or acknowledge the help you got from others during your research work.

8 References

[1] Adil, Syed Hasan, et al. "3D smart city simulator." Robotics and Manufacturing Automation (ROMA), 2017 IEEE 3rd International Symposium in. IEEE, 2017. https://doi.org/10.1109/ROMA.2017.8231826

[2] Saloni, Matteo, et al. "Lasso: A device-to-device group monitoring service for smart cities." Smart Cities Conference (ISC2), 2017 International. IEEE, 2017. https://doi.org/10.1109/ISC2.2017.8090796

[3] Loriot, Marine, Ammar Aljer, and Isam Shahrour. "Analysis of the use of LoRaWan technology in a large-scale smart city demonstrator." Sensors Networks Smart and Emerging Technologies (SENSET), 2017. IEEE, 2017. https://doi.org/10.1109/SENSET.2017.8125011

[4] Gyayak Sanghi Nalin Kanungo Sagar Deshmukh Sonali Agarwal, 978-1-5090-6255-3/17/$31.00 Â©2017 IEEE.

[5] Khatavkar, Nikhil, A. A. Naik, and Balaji Kadam. "Energy efficient street light controller for smart cities." Microelectronic Devices, Circuits and Systems (ICMDCS), 2017 International Conference on. IEEE, 2017. https://doi.org/10.1109/ICMDCS.2017.8211714

[6] Rivera, Rogelio, et al. "How digital identity on blockchain can contribute in a smart city environment." Smart Cities Conference (ISC2), 2017 International. IEEE, 2017. https://doi.org/10.1109/ISC2.2017.8090839
[7] Velladurai, V. S., et al. "Human safety system in drainage, unused well and garbage alerting system for smart city." I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on. IEEE, 2017. https://doi.org/10.1109/I-SMAC.2017.8058319
[8] Dalla Cia, Massimo, et al. "Mobility-aware handover strategies in smart cities." Wireless Communication Systems (ISWCS), 2017 International Symposium on. IEEE, 2017. https://doi.org/10.1109/ISWCS.2017.8108155
[9] Amit Dua, Neeraj Kumar, Ashok Kumar Das, and Willy Susilo. Secure message communication protocol among vehicles in smart city. IEEE Transactions on Vehicular Technology, 2017 Dec 12. https://doi.org/10.1109/TVT.2017.2780183
[10] Zhu, Chunsheng, et al. "Secure multimedia big data in trust-assisted sensor-cloud for smart city." IEEE Communications Magazine, vol. 55, no. 12, pp. 24–30, 2017. https://doi.org/10.1109/MCOM.2017.1700212
[11] Kanase, Pooja, and Sneha Gaikwad. "Smart hospitals using internet of things (IoT)." International Research Journal of Engineering and Technology (IRJET), 3, 1735–1737, 2016.
[12] Vappangi, Suseela, and Venkata Mani Vakamulla. "Synchronization in Visible Light Communication for Smart Cities." IEEE Sensors Journal (2017). https://doi.org/10.1109/JSEN.2017.2777998
[13] Sfikas, Giorgos, Charilaos Akasiadis, and Evaggelos Spyrou. "Creating a Smart Room using an IoT Approach."
[14] Dalla Cia, Massimo, et al. "Using smart city data in 5G self-organizing networks." IEEE Internet of Things Journal (2017). https://doi.org/10.1109/JIOT.2017.2752761
[15] Wang, Jingjing, et al. "Vehicular sensing networks in a smart city: Principles, technologies and applications." IEEE Wireless Communications, vol. 25, no. 1, 122–132, 2018. https://doi.org/10.1109/MWC.2017.1600275
[16] Benltoufa, Ahmed Noureddine Helal Sofien, et al. "From smart campus to smart city: Monastir living lab." Engineering and Technology (ICET), 2017 International Conference on. IEEE, 2017. https://doi.org/10.1109/ICEngTechnol.2017.8308196
[17] Lin, Chia-Ying, et al. "Utilization-based parking space suggestion in smart city." Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual. IEEE, 2018. https://doi.org/10.1109/CCNC.2018.8319281
[18] Beigi, Nazli Khan, Bahar Partov, and Soodeh Farokhi. "Real-time cloud robotics in practical smart city applications." Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on. IEEE, 2017. https://doi.org/10.1109/PIMRC.2017.8292655
[19] Kodali, Ravi Kishore, and P. Siva Ramakrishna. "Modern sanitation technologies for smart cities." Humanitarian Technology Conference (R10-HTC), 2017 IEEE Region 10. IEEE, 2017. https://doi.org/10.1109/R10-HTC.2017.8289055
[20] Hugh Boyes. Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review, vol. 5, no. 4, 28, 2015. https://doi.org/10.22215/timreview/888
[21] Bhide, Vishwajeet, H. "A survey on the smart homes using internet of things (IoT)." International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 12, 243–246, 2014.
[22] Pribadi, Arif, et al. "Urban distribution CCTV for smart city using decision tree methods." Intelligent Technology and Its Applications (ISITIA), 2017 International Seminar on. IEEE, 2017. https://doi.org/10.1109/ISITIA.2017.8124048
[23] Jeong, Hyewon, et al. "A low-power high-performance SoC platform for IoT applications." (2016).

[24] Latif, Saba Latif, Hamra Afzaal Afzaal, and Nazir Ahmad Zafar. "Modeling of sewerage system using internet of things for smart city." Frontiers of Information Technology (FIT), 2017 International Conference on. IEEE, 2017. https://doi.org/10.1109/FIT.2017.00016

[25] Suri, Bhawna, et al. "Smart threat alert system using IoT." Computing, Communication and Automation (ICCCA), 2017 International Conference on. IEEE, 2017. https://doi.org/10.1109/CCAA.2017.8230006

[26] Castillejo, Pedro, et al. "An internet of things approach for managing smart services provided by wearable devices." International Journal of Distributed Sensor Networks, vol. 9, no. 2, 190813, 2013. https://doi.org/10.1155/2013/190813

[27] Florez, Daniel, and Johanna Sepulveda. "BlooXY: On a non-invasive blood monitor for the IoT context." System-on-Chip Conference (SOCC), 2017 30th IEEE International. IEEE, 2017. https://doi.org/10.1109/SOCC.2017.8226000

[28] Sundar, Ganesh Venkat, and Balaji Ganesh Rajagopal. "IoT based passenger information system optimized for Indian metros." Electronics, Communication and Aerospace Technology (ICECA), 2017 International Conference of. vol. 1. IEEE, 2017. https://doi.org/10.1109/ICECA.2017.8203650

[29] Kök, İbrahim, Mehmet Ulvi Şimşek, and Suat Özdemir. "A deep learning model for air quality prediction in smart cities." Big Data (Big Data), 2017 IEEE International Conference on. IEEE, 2017.

[30] Haider Th.Salim Alrikabi and Hussein Tuama Hazim, "Enhanced data security of communication system using combined encryption and steganography," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 16, 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[31] Abdul Hadi Alaidi, Chen S Soong Der, and Yeng Weng Leong, "Systematic Review of Enhancement of Artificial Bee Colony Algorithm Using Ant Colony Pheromone," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 16, 173, 2021. https://doi.org/10.3991/ijim.v15i16.24171

[32] Haider Th. Salim Alrikabi and Nabaa Ali Jasim, "Design and implementation of smart city applications based on the internet of things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 13, 4–15, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[33] Sikder, Amit Kumar, et al. "IoT-enabled smart lighting systems for smart cities." Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual. IEEE, 2018. https://doi.org/10.1109/CCWC.2018.8301744

9 Author

Prof. Dr. Karl Brown, College of Computer sciences, Texas Tech University, USA.

Article submitted 2022-02-07. Resubmitted 2022-03-10. Final acceptance 2022-03-11. Final version published as submitted by the authors.