An adaptable cell load estimation and energy management method based CRN with generative adversarial network (GAN) for 6G and beyond 6G

M JANAKI RAMAN,
Departmnet of CSE,
Rrase College of Engineering,
Chennnai

Mr Ragaganapathy.G
Assistant Professor
Rrase College of Engineering,
Chennnai

Dr. K. RAVIKUMAR
Professor, Department of Cse
Rrase College of Enginnering
Chennai

Abstract:

Communication requirements for the cognitive radio networks need novel solutions, to overcome the limitations of dynamic spectrum access. In this regard, the hybrid enhanced adaptive acknowledgement (HEAACK) was introduced at the mobile Internet Protocol (IP) layer to allow cognitive mobile users to use their channel as long as possible, to avoid any increase in interruption loss due to unnecessary channel adaptations. . In this paper, the Transport-layer (TCP) performance is examined with the HEAACK application, to evaluate the TCP/IP interface effects and to analyses the performance on congestion control and capacity utilization.

1. INTRODUCTION

The rapid growth in the ubiquitous wireless services has imposed increasing stress on the fixed and limited radio spectrum. Cognitive mobile users are inquiring on-time access to high speed data for real-time services, as part of efficient services..

Accordingly, extensive measurements reported indicate that the static frequency allocation results in a low utilization (only 6%) of the licensed radio spectrum most of the time. The adaptation between different channels, named Spectrum Handover (SH), adds another factor of time delay experienced by cognitive users, especially vehicular mobiles. Unlike traditional wireless networks, which typically occupy contiguous bands, a cognitive radio network is expected to operate over a set of highly separated non-contiguous frequency bands, which exhibit different RF attenuation and interference behaviors. It is well known that signal attenuation increases with the distance between the two communicating users and also with the carrier frequency used for communication.

Therefore, when assigning channels for its transmissions, it is necessary for a cognitive radio network to try to select the "best" set of channels for a given transmission.

The fifth generation (5G) and beyond 5G (B5G) LTE system wireless networks face challenges. Wireless communication systems have experienced substantial revolutionary progress over the past years. With the rapid progress of 3GPP 5G phase 2 standardization, the commercial deployment of 5G applications being deployed all over the world cannot fully meet the challenges brought by the rapid increase of traffic and the real-time requirement of services

OBJECTIVE: The main objective of the system is to reduce the network interference between two networks and to find the shortest path between two end points. This will enable a secure and intercepted communication.

EXISTING SYSTEM: In the face of the user-centric access network architecture adopted by the fifth-generation (5G) mobile communication network terminals, the communication capability of terminals faces significant challenges

DISADVANTAGES:

- Cannot predict the load estimation on the access side of the network in advance.
- Throughput is low.
- Path oscillation gets highly oscillated.
- Congestion will be occurred.
- Energy loss is very high.

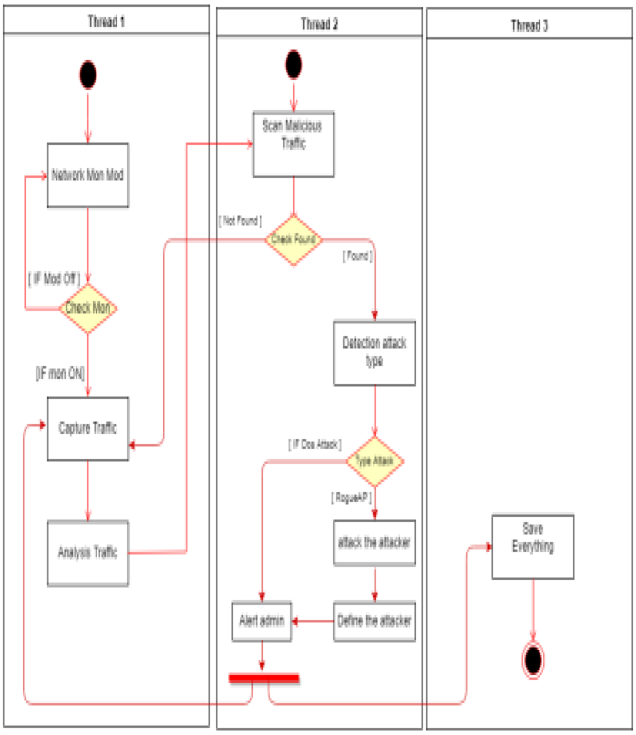
PROPOSED SYSTEM:

This system is based on collecting data traffic from "management frames" which are specific to wireless networks that work within IEEE 802.11 frequency. The users send this frequency within the company, then these data are analyzed using a specific system. After that these data could be classified into two categories: normal and suspicious actions. In both cases the system continues to do in analysis every 20 seconds, but if the action is suspicious the system will take extra steps in parallel with these basic steps. The system will take an action against the attacker -if the type of attack allows that- then we can determine the location of the attacker. The system analyzes the users' behavior and the networks that they are using. In addition, the system updates the system's database. All these actions are supervised by the system's administrator.

ADVANTAGES:

- It establishes route on demand.
- It create loop free nodes.
- It maintains connectivity
- Fast and efficient recovery from failures.

ARCHITECTURE DIAGRAM



2. LITERATURE SURVEY

1. Self-optimization of cellular networks using deep reinforcement learning with hybrid action space

Wireless networks have been going through tremendous proliferation recently. As a result, a continuous configuration and management are necessary to sustain a balanced performance while facing such continued growth and endless changes.

ADVANTAGES:

1. Throughput is improved.
2. Congestion of packet transmission, receiption; gets minimized.
3. Easy to implement.

DISADVANTAGES:

1. Throughput is low.
2. Path oscillation gets highly oscillated.
3. Congestion will be occurred.

2. Enhanced mobility load balancing algorithm for 5G small cell networks

The mobility load balancing is introduced to avoid the quality of service degradation due to imbalanced load through small cells of the network.

ADVANTAGES:

1. Critical situation of flooding is predicted.
2. Routing process didn’t need location information.
3. It can equalize energy consumption.

DISADVANTAGES:

1. A lower propagation speed.
2. Longer delay.
3. Lower delivery rate.

3. Toward the standardization of non-orthogonal multiple access for next generation wireless networks

Non-orthogonal multiple access (NOMA) as an efficient method of radio resource sharing has its roots in network information theory.

ADVANTAGES:

1. It establishes route on demand.
2. It creates loop free nodes.
3. It maintains connectivity.

DISADVANTAGES:

1. The network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail.
2. More seriously.

Make incorrect decisions

4.Multiple Access Techniques for 5G Wireless Networks and Beyond:

This article presents comprehensive coverage of current and emerging multiple access, random access, and waveform design techniques for 5G wireless networks and beyond.

ADVANTAGES:

1. Has better packet delivery ratio
2. Comparatively low average end-to-end delay
3. Starvation is reduced in the networks.

DISADVANTAGES:

1. Throughput is low.
2. Handover delay will be occurred.
3. Energy is wasted during hand over.

MODULE DESCRIPTION:

MODULES NAMES:

- **CELL LOAD ESTIMATION**
- **Route Discovery**
- **Signaling and Link Establishment**

CELL LOAD ESTIMATION:

Introduce a HEAACK by which we can provide efficient bandwidth utilization by all the nodes in a network and provide fairness in a network. To evaluate the data rate, packet size for cell load estimation. The types of traffic to analyze the level of starvation such that the non-necessary adjustments are reduced. A short time to reduce the channel occupancy time. Namely, the nodes with short signal strength still has chance to send out the packets. Small packet size with low transmission frequency can be finished in a short time to reduce the level of starvation. High packet size with high transmission frequency can be finished in a short time by MPTCP channels.

Route Discovery:

When a source attempts to send a packet to a destination, it checks its routing table first. If there is not an entry for the destination, the route discovery process starts.HEAACK: In MPTCP, the forwarded control packets include RREQ (Route Request), BRREQ (Backward Route Request), RREP (Route Repay), and RERR (Route Error). During the first path discovery (generator function of GAN), the intermediate node information list contained in RREQ consists of ID and geographic information of the nodes in the first established path. During the second path discovery (discriminator), BRREQ piggybacks the intermediate node list of the first path and chooses the nodes in the second path away from the first path.

Signaling and Channel Establishment:

Once the topology transition sequence has been determined, the new transceiver pairs prepare to form a new link. This includes breaking the existing channel, notifying the network and higher layers of the broken and new links, and exchanging handshake messages to form the new channel. It is assumed that the sequencing scheme will establish a set of channel to allow provisioning of primary paths carrying live traffic first and then establish the remaining channel to allow the provisioning of non-traffic-carrying channels and the secondary and higher-order restoration paths. The establishment of channel supporting the restoration paths will, in general, be done using the same methods used by primary channel formation. The link establishment step involves pointing and tracking, adjusting transceiver compatibility, invoking performance monitoring of the channel, and optimizing channel quality. When the new transceiver pairs establish a stable channel they communicate the new channel information to the network and to the control and management planes of the higher layers.

PROPOSED ALGORITHM:

This system is based on collecting data traffic from "management frames" which are specific to wireless networks that work within IEEE 802.11 frequency. The users send this frequency within the company, then these data are analyzed using a specific system. After that these data could be classified into two categories: normal and suspicious actions. In both cases the system continues to do in analysis every 20 seconds, but if the action is suspicious the system will take extra steps in parallel with these basic steps. The system will take an action against the attacker -if the type of attack allows that- then we can determine the location of the attacker. The system analyzes the users' behavior and the networks that they are using. In addition, the system updates the system's database. All these actions are supervised by the system's administrator.

In case of monitoring, the Supervisory system controls, analyses and classify the data that flow to the system. In addition if there is an attack on the system the supervisory system is responsible for saving the network and sending warning signs if there is any abnormal behavior. The system will record data traffic in the bandwidth, then analyses these data and save the results of the analysis. After that the system will present the results of the analysis including the networks that surrounding the institution, which is followed by classification of these waves based on their behavior into two categories:

Threat identification (By middle bandwidth)

The first step in designing and building any defense system is to identify security threats that we want to monitor or exactly want from an intrusion detection system, because there is no system that **detects all known attack types or zeroday attacks. After identifying** and classifying the external risks of the system, start identifying the sources and places of internal danger, we can then determine which parts are under threat and what type of threat we may have to start building an intrusion detection system that meets our basic requirements of monitoring and protecting these parts within the network. All these procedures will eventually make the system stable and effective and help system administrators instead of jamming them by significantly reducing the false warnings.

Data Collection (Storage Phase)

After identifying internal and external risks well and what things we should be concerned about, we move on to the second step which is the step on what data to collect. Since we have determined that there is a potential risk within the network or from authorized or unauthorized persons this means collecting information from suspicious or normal activities of data traffic on the external and internal networks. It is very important to improve the standards and priorities of wireless intrusion detection systems. These standards will play an important role in measuring attacks on the network and build our own standards that meet our system needs. We have to include our standards for everything that the system needs to meet our requirements. Collecting massive information and analyzing it is due to the lack of reliable measures. If there is a specific danger we should be aware of in a wireless world is the behavior of the network and users who are the only factor that governs whether there is a danger or not.

For example, important data collected to analyze network behavior and users are as follows:

● Service type

● Service count

● Source

● Destination

● Logged in

● Dst_host_count

● Packet count

● Dst_host_srv_count

Detection strategy (sensing low bandwidth in channels)

Once priorities are determined and what attacks are most important to us, then another step is taking apart now which is the detection strategy. The detection strategy is one of the main tasks of the defense system and relies closely on the information gathering process that will be given to the detection strategy to determine what malicious behavior nor normal behavior. Since there is a huge amount of data flow within the wireless networks, it makes sense that this process will be difficult and impossible to human, so this process must be done automatically through the computer, which we do through the development of certain controls for the movement of data to the network, Anomalies in the network. For example, after collecting data flow in bandwidth, analyzing WIFI management frames, and calculating the number of requests received by a particular router, we can then judge that our network is experiencing denial of service attacks. All these controls must be strictly enforced by having a precise vision of what will happen to the network so that we go beyond false positives. This stage is extremely sensitive to any error in which the system will be built to defend our network as our enemy and prevent our access to network sources.

Digital Forensics (Investigation phase -High level bandwidth)

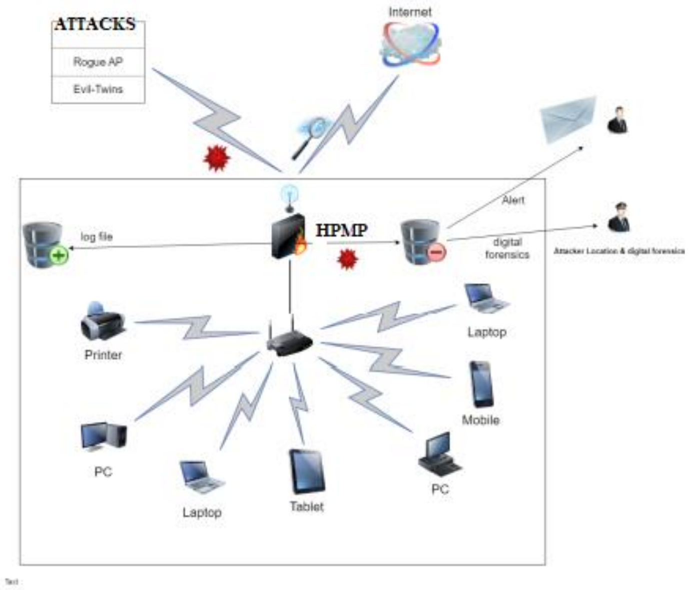
Networks in all their forms are at risk of cyber-attacks and a primary target for cybercriminals. Therefore, such attacks must be investigated in the same way as any crime. In the digital world, digital forensic science is responsible for providing such evidence for submission to courts. The main advantage of digital forensics is to obtain evidence of attacks that the system has failed to block so that the human element can intervene to improve the level of security in the network. Digital forensics is a very complex field of research and has many difficulties, particularly in the wireless network environment because of the nature of these variable and mobile networks. 802.11 is the main source of information in the wireless intrusion detection system. After identifying the risks and gathering the appropriate information and identifying the strategies of detecting the attack, the important role in this system is the process of analyzing the attack and behind the attack and analyzing all the data available to reach the evidence of the party responsible for the attack. Digital forensics medicine plays a large and effective role in the analysis of attack and the application of the principles of this science well gives the opportunity to predict future attacks in the future by examining the intentions of the attackers and targets of their breakthrough and gives us a vision of the most parts of the system targeted.

However, at the information gathering stage, we have gathered the appropriate information for us to use in the digital criminal investigation process.

The investigation into the system was divided into three sections:

1. First, investigate the Rogue AP networks and identity of the attacker 2. Investigate through the MAC address of devices that are trying to communicate with our network 3. Digital investigation of user behavior

PROPOSED HPMP IN WIRELESS SENSOR NETWORK



CONCLUSION

Attackers exploits in channel to selectively drop packets, to build bogus route information, to create routing loops to waste the energy of network, to gain unauthorized access, to disrupt routing, to perform denial of service attacks, to blackmail a good node and induce rushing attack. In this paper, the attackers selectively drop packet, replays the data packets, gain unauthorized access and transmit data packets at high energy. The implemented solution of “Secure Routing Algorithms for Detecting and preventing of Attacks in Wireless Sensor Networks” solves the problem of this resource consumption multi attacks that is induced by creating channel holes in the wireless sensor networks. Preventing these attacks solves the problem of routing the legitimate packets in the dysfunctional way.

REFERENCES:

[1] Jin-Yong Yu, Euijong Lee, Se-Ra Oh, Young-Duk Seo and Young-Gab Kim, "A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security", IEEE Access, 2020.

[2] Christian Miranda, Georges Kaddoum, Elias Bou-Harb, Sahil Garg and Kuljeet Kaur, "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 2020.

[3] Muhammad Nawaz Khan, Haseeb Ur Rahman, Mohammed Amin Almaiah, Muhammad Zahid Khan and Ajab Khan, "Improving Energy Efficiency With ContentBased Adaptive and Dynamic Scheduling in Wireless Sensor Networks", IEEE Access, 2020.

[4] Boubiche, D.E., Athmani, S., Boubiche, S. et al. Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions. Wireless Pers Commun 117, 17213(2021).https://doi.org/10.1007/s11277-020-07213-5.

[5] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni and Yinxuan Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey", Hindawi, Wireless Communications and Mobile Computing, 2020.

[6] Vikhyath K B and S.H. Brahmanand, "Wireless sensor networks security issues and challenges: A survey", International Journal of Engineering & Technology, 2018.

[7] Jianming Liu, Ziyan Zhao, Jerry Ji and Miaolong Hu, "Research and application of wireless sensor network technology in power transmission and distribution system", Intelligent and Converged Networks, 2020.

[8] Khalid Haseeb, Khaled Mohamad Almustafa, Zahoor Jan, Tanzila Saba and Usman Tariq, "Secure and

Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network", IEEE Access, 2020.

[9] Zusheng Zhang, Xufei Mao, Kunxiao Zhou and Huaqiang Yuan, "Collaborative Sensing-Based Parking Tracking System With Wireless Magnetic Sensor Network", IEEE Sensors Journal, 2020.

[10] Van Nhan Vo, Tri Gia Nguyen, Chakchai So-In and DacBinh Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer", IEEE Access, 2020.

[11] Chen, Joy Iong Zong. "Optimal Multipath Conveyance with Improved Survivability for WSN's In Challenging Location." Journal of ISMAC 2, no. 02 (2020): 73-82.

[12] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." Journal of ISMAC 2, no. 02 (2020): 106-117.

[13] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, " A Survey of Wireless Sensor Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[14] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Wireless Sensor Network ,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[15] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002. [9]. 6Khin Sandar Win," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.