International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

MISBEHAVIOUR NODE PREDICTION BY USING STATE MACHINE ALGORITHM IN COGNITIVE RADIO NETWORK

S.P.Anitha[1], P.Ilanchezhian[2]

[1]*PG Scholar, Dept. Of Information Technology, Sona College of Technology, Tamilnadu, India*
[1]*anithapalanisamydce@gmail.com*
[2]*Asso Professor, Dept. Of Information technology, Sona College of Technology, Tamilnadu, India.*
[2]*nibiila@yahoo.co.in*

----------***----------

Abstract- *Anomaly based intrusion detection system for IEEE 802.11 wireless networks based on behavioral analysis by detecting deviations which behaves normally that are triggered by wireless network attacks. The system uses a set of rules and signatures to model the malicious activities and attacks. An alarm is generated whenever those rules are triggered or attack signatures are detected. In addition it has been verified that the proposed approach has a good tolerance against frame loss which is a common issue in wireless networks which can happen due to mobility of the nodes or traffic congestion. The main contribution of this paper is that it introduces an anomaly behavioural analysis methodology and intrusion detection system in cognitive radio network. Since our methodology is based on partially modelling of the protocol state machine, it can be easily applied to other protocols such as ZigBee, Bluetooth, and cognitive network etc. To enhance the attacks specific to CR (Cognitive Radio) networks, we observe that a common characteristic of attacks in both examples is that in which they cause anomalous spectrum usage and disrupt the dynamic spectrum access thus we termed them as "Anomalous Spectrum Usage Attacks" (ASUAs) in the context of CR wireless networks.*

Keywords: **Anomaly detection, IEEE 802.11 security, Intrusion detection, Wireless Network security, Protocol analysis**

1. INTRODUCTION

Wireless technology have the most widely used communication medium, both in home and enterprise networks. The main advantages of wireless networks versus wired networks are their mobility, we can categorize the available Wireless Intrusion Detection Systems (WIDS) [6] according to the reference data or the analysis techniques. According to the reference data we can group the Wireless IDSs into three groups: those which focus on the physical layer data. Those which use the data link layer (MAC layer) data and the ones which combine the information from both layers. In this paper, we present a Wireless LAN (IEEE 802.11) Intrusion Detection System (IDS) based on anomaly behaviour analysis of the MAC layer frames with high detection rate and low false alarms. The system builds online models from the state machine transitions of the IEEE 802.11 during its normal operation, and it flags any significant deviation from these state machine transitions as an abnormal activity. To generate the normal transition models, the system extracts any n consecutive state-machine transitions as an n-gram pattern and stores these extracted patterns as a normal model. At runtime, the [5] IDS system matches the monitored n-grams of the real traffic sessions with the normal transition model in order to detect any abnormal sessions. The provider would offer the service for a charge probably on a pay per use system, and the client would be able to take favourable of this service in an active location; away from the office or home. A drawback of wireless Internet is that the QoS (Quality of Service) [5] is not assurance and if there is any interference with the link then the connection may be dropped.

2. RELATED WORK

2.1WLAN Standard IEEE 802.11

Wireless networks versus wired networks are their mobility, flexibility and inexpensive deployment and maintenance cost, especially in places that wiring is difficult. With the exponential growth in the deployment of Wireless Local Area Networks (WLAN),[5] the security issue of these networks has become a major concern for both users and providers. The performance, the IEEE 802.11 standard was dedicated to security amendments. Despite IEEE 802.11i has provided good mechanisms to improve privacy and confidentiality, it still does not provide enough protection for availability and integrity.

IEEE 802.11n, the most recent version of IEEE 802.11, is shipping in volume; the focus is on with high speed solutions, specifically IEEE 802.11ac and IEEE 802.11ad. The aim to provide gigabit speed WLAN. IEEE 802.11s is an IEEE 802.11 amendment for mesh networking, describe how wireless devices can connect with each other to create a WLAN mesh network, which may be used for ad hoc networks and static topologies. 802.11 is a set of IEEE standards that govern wireless networking transmission methods.

2.2 INTRUSION DETECTION SYSTEMS (IDSS)

An intrusion detection system monitors [7] network traffic and monitors for alerts and suspicious activity for the network administrator or system. In some cases the intrusion detection system may also respond to malicious or anomalous traffic by taking action such as blocking or source IP address or user from accessing the network.

Intrusion detection system approach the goal of detecting unsure traffic in contrasting ways. There are network based and host based intrusion detection systems. There are intrusion detection system that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically discover and protects against malware- and there are intrusion detection system that identify based on comparing traffic marking against a baseline and looking for anomalies.

Intrusion detection functions include, analyzing and Monitoring both system and user activities, Analyzing vulnerabilities, system configurations Assessing system and file integrity, Analysis of abnormal activity patterns, Ability to recognize patterns typical of attacks, tracking user policy violations. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming knowledgeable, less technical ability is required for the novice attacker, because existing methods are easily accessed through the Website.

3. PROPOSED WORK

CSMA/CA at the Medium Access Control (MAC) [8] layer that has a predecided Common Control [10] Channel (CCC) for coordination of the spectrum band and channel during data transfer. Use a priority queue, Qp at the MAC layer for the TCP CRAHN control packets, also be drawn from in between positions in Qp. In a CR network, nodes maintain a list of unoccupied channels that may belong to different spectrum bands. In our work set of channels is identified through spectrum sensing, handle during the back off meantime following a packet transmission or reception at the link layer. On the current [9] operational channel, an accurate idea of the PU activity. For this, we do not rely on sensing times. Rather, nodes sense their present channel for the sensing time at regular intervals at the cost of continued network connection.

- Normal
- Spectrum sensing
- Spectrum change
- Mobility predicted
- Connection establishment
- Route failure

3.1 CONNECTION ESTABLISHMENT

TCP CRAHN modifies the three-way handshake in TCP new Reno so that the source can get the sensing list of the nodes in the routing path. First, the source sends out a Synchronization packet to the destination.

An in-between node, say i, in the routing path appends the following information to the SYN packet: 1) the tuple, 2) a timestamp, and 3) its ID. The time left before the node starts the next round of spectrum sensing, [2] calculated from the timestamp is the constant time between two successive spectrum sensing events, and stir is the time taken to finish the sensing in the present cycle. On receiving the SYN packet, the receiver sends a SYN-ACK message to the source. The sensing data's gathered for each node is piggybacked over the SYN-ACK and the source knows when a node in the way shall undertake spectrum sensing and its duration. The final ACK is then sent by the source to the sink completing the handshake.

3.2 NORMAL STATE

The normal state in [1] TCP CRAHN is the usual state and resembles the long established functioning of the classical TCP new Reno protocol. Our protocol enters this state when 1) there are no connection breaks due to PU arrivals, 2) no node in the path is currently engaged in spectrum sensing and 3) no close route failure is signaled. Thus, the path to the destination remains connected and ACKs sent by the closing are collect at the source. The contrast between TCP CRAHN in the normal state and the classical TCP are as follows. Feedback through the ACK the in between nodes of the path piggyback the following link-layer information over the data packets to the sink, which is then sent to the source through ACKs. Residual buffer space (Bfi). Consider a node i that has Bui unoccupied buffer space. Let the number of flows passing through it be nfi. The fair share of the residual buffer space per flow. Observed link bandwidth each node i maintains a weighted average of the perceived bandwidth on the link formed with its next hop during the normal state. This is obtained from the link layer as the ratio of the acknowledged information bits to the time taken for this transfer between the nodes.

3.3 SPECTRUM SENSING STATE

TCP CRAHN [1] adapts to spectrum sensing through 1) flow control, which prevents buffer overflow for the intermediate nodes during sensing and 2) regulating the sensing time to meet the specified throughput demands the aim of TCP CRAHN is to alter the flow control mechanism.

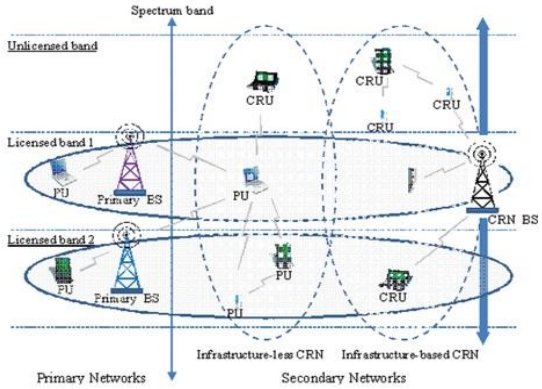

Figure 3.3Spectrum Sensing

In TCP, the node prior to the sensing node is not buried with arriving data packets. If another node j has an overlapping sensing schedule, TCP CRAHN [3] uses the residual buffer space of the previous hop of the node closest to the source during the period of extend over, say i. When the sensing time of the neighbor node is completed, the buffer space of node j is used in the end computations the maximum number of bytes of unacknowledged information allowed at the sender is the minimum of the present congestion window, and the receive window showed by the destination, rwind. The rwind represents the free space in the destination's buffer that can accommodate extra transmitted packets. During the sensing duration, no ACKs are received by the source and hence the rwind remains unchanged. This also results in a constant cwnd as TCP is self-clocked and does not enlarge in the non-appearance of the receiver ACK. The effective window, ewnd at the sender is modified to include an estimate of the free buffer space, Bf.

3.4 SPECTRUM CHANGE STATE

In the ideal case, the effective bandwidth of the TCP [5] connection is dependent on several factors, such as contention delays and channel errors at the link layer, apart from the raw bandwidth of the channel. In this section, we show how TCP CRAHN [1] scales its cwnd rapidly, say from point B to a different value B'.

Its then sends back a link layer ACK [7] to node i to inform the node of its choice. All the coordination up to this point occurs on the old channel. A second set of Problem and ACK messages are then exchanged on the channel to be switched, a confirmation and also to approximately estimate the new link transmission delay times Li; i_1 and Li_1.

3.5 MOBILITY PREDICTED STATE

In order to address the problem of delayed route failure notification a mobility prediction framework based on Kalman filter-based estimation, which uses the [4] Received Signal Strength (RSS) information from the link layer. The set of Kalman equations similar to the disposition for calculating sensor location but for a simpler, scalar case of a single dimension of the received power value. The nodes of the path monitor the connectivity to their next hop downstream node by measuring the [4] RSS of the ACKs and the periodic beacon messages. At each epoch, the prediction value is compared with the minimum RSS required for receiver operation. If the condition of possible link failure is predicted in the next epoch, the destination is informed, which then sets the Mobility Flag (MF) in the outgoing ACKs. The source responds to this by limiting the cwnd to the ssthresh and the congestion avoidance phase is never initiated. The aim of this adjustment, cwnd _ ssthresh, is to limit the number of packets injected into the route which has a possibility of an outage, as the CR specific function of the nodes may delay the arrival of the actual link failure notification. If no ICMP message is received at the source subsequently, signaling that a route failure has indeed occurred or the incoming ACKs do not have the MF flag sent, the mobility prediction state is cancelled and TCP CRAHN reverts back to the state.

3.6 ROUTE FAILURE STATE

The node i sends a destination unreachable message in the form of an ICMP [6] packet if 1) the next hop node i - 1 is not reachable based on link layer retries, 2) there is no ongoing spectrum sensing based on the last known schedule, and 3) no EPN [1] message is received at node i signaling a temporary path disconnection due to PU activity. At this stage, the source stops transmission and a fresh connection needs to be formed over the new route by TCP CRAHN.

4. SIMULATION AND RESULT

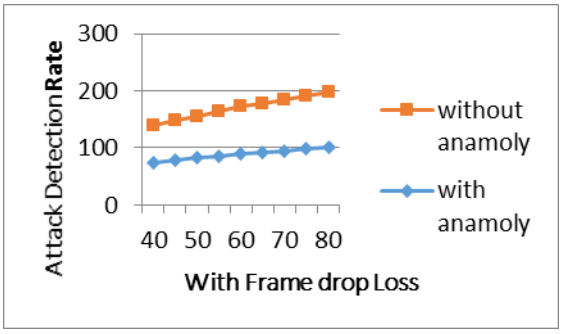

Figure-1: Packet Delivery Ratio

The figure 1 depicts the packet delivery ratio of the system existing and with state machine algorithm. As compared with the number of nodes in x-axis and PDR in y-axis it is proved that ratio has been increased with the use of algorithm.

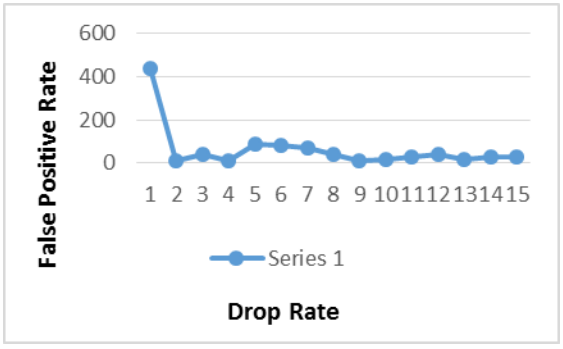

Figure-2: False Positive Rate with Frame Loss

The figure 2 in which the frame loss tolerance is that the system is trained based on normal network traffic which includes the normal frame loss scenarios due to congestion or mobility. In addition, in cognitive network MAC protocol a frame will get retransmitted up to a certain number of times if it is lost due to random channel errors.

5. CONCLUSION

Radio behavior and potential security threats in cognitive radio networks are investigated in order to successfully deploy CR networks and realize its benefits. A complex CR misuse issues during its secondary access processes, including misbehavior, cheating, and attack is determined. A new type of cognitive attack, most active band (MAB) attack, is introduced in this system, where an attacker or a malicious CR node senses/determines the most active band within a multi-band Cognitive Radionetwork and targets this band through a denial of service attack.

REFERENCES

[1] A. Capone, L. Fratta, and F. Martignon (2004), "Bandwidth Estimation Schemes for TCP over Wireless Networks," IEEE Trans. MobileComputing, vol. 3, no. 2, pp. 129-143.

[2] A.O. Bicen and O.B. Akan (2011), "Reliability and Congestion Control in Cognitive Radio Sensor Networks," Ad Hoc Networks J., vol. 9, no. 7, pp. 1154-1164, Elsevier.

[3] G. Holland and N.H. Vaidya (1999), "Analysis of TCP Performance over Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 219-230.

[4] I.F. Akyildiz, W.Y. Lee, and K. Chowdhury (2009), "CRAHNs: Cognitive Radio Ad Hoc Networks," Ad Hoc Networks J., vol. 7, no. 2, pp. 810-836, Elsevier.

[5] J. Liu and S. Singh (2001), "ATCP: TCP for Mobile Ad Hoc Networks," IEEE J. Selected Areas of Comm., vol. 19, no. 7, pp. 1300-1315.

[6] K.Chen, Y. Xue, and K. Nahrstedt (2003), "On Setting TCP's Congestion Window Limit in Mobile Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 1080-1084.

[7] K.R. Chowdhury, M. Di Felice, and I.F. Akyildiz (2009), "TP-CRAHN: A Transport Protocol for Cognitive Radio Ad Hoc Networks," Proc. IEEE INFOCOM, pp. 2482-2491.

[8] L. Brakmo and L. Peterson (1995), "TCP Vegas: End to End Congestion Avoidance on a Global Internet," IEEE J. Selected Areas in Comm. vol. 13, no. 8, pp. 1465-1480.

[9] M. Di Felice, K. Chowdhury, W. Kim, A. Kassler, and L. Bononi (2011), "End-to-End Protocols for Cognitive Radio Ad Hoc Networks: An Evaluation Study," Performance Evaluation, vol. 68, no. 9, pp. 859- 875.

[10] M. Di Felice, K.R. Chowdhury, and L.Bononi (2009), "Modeling and Performance Evaluation of Transmission Control Protocol over Cognitive Radio Ad Hoc Networks," Proc. 12th ACM Int'l Conf. Modeling, Analysis and Simulation of Wireless and Mobile (MSWIM '09), pp. 4-12