Advanced Research Topics in Computer Science

7COM1084

Name: Ashwani Sharma

Student ID: 20010267

PART 1: CYBER SECURITY SPECIALISM

INTRODUCTION

Wireless networking is becoming increasingly popular, and as a result, security has risen to the top of the priority list for businesses of all sizes. Security protocols and key exchange methods in IEEE 802.11 networks have received a lot of attention recently. These networks, on the other hand, are nevertheless vulnerable to probe request assaults since these attacks typically occur before security procedures are activated (Robinson, F., 2004.). Availability factor in the security protocol is impacted by probe request attacks. In order to prevent legitimate clients from accessing resources, probe request attacks are commonly used. Rogue access points, for example, can be introduced using this attack which may lead to loss of users information. Wireless security research has thus far concentrated mostly on protecting networks' confidentiality and integrity, with little consideration paid to these attacks. Probe request attacks on wireless networks have grown in popularity as a result of the widespread usage of IEEE 802.11 wireless networks in both residential and commercial settings. Despite this, there is no viable remedy to these issues (Guo, F. and Chiueh, T.C., 2005).

OPEN RESEARCH QUESTIONS

APs that receive a probe request frame must reply with a suitable probe response frame, which provides information about the network, to enable the station to connect. As these probe requests are done without any encryption anyone in the range of signal can view the information on the request. Attackers monitor these requests for finding out information about the other devices and also effect the performance of the router (Tippenhauer, N.O., et al,2009). They can create a denial-of-service attack or make accessing resources more difficult effecting the genuine users. This problem is solved by the research by using the neural networks to predict the real and fake users by looking like the frames data.

The research question which has been examined is “how does the intelligent system prevent the probe request attacks”. This is an interesting question as most of the security research are focused on protecting the users after connecting to the device. Which make opportunity for the intruders to plan malicious attacks doS, spoofing and many more. This research has many real time use cases as Wi-Fi is used in public places where the intruder can plan an attack and effect all the people connecting to it (Ratnayake, D.N., et al,2011).

Geetha, K. and Sreenath, N., in 2014 conducted an analysis of flooding attacks and their impacts on the network. This research shows how the attacks can affect the performance of the system by occupying the resources. A denial-of-service assault is discovered via the use of an identification test, which is described in this work. Prior to and after an assault, the most critical parameters for message transport are examined. Only by examining the numerous criteria can the attack's existence be established. Hence these states various parameter needs to be analysed in the network before performing analysis which was done in the paper. Proving its significance.

EXISTING AND RELATED WORK:

An ANN is a computer programme that simulates the workings of a human brain. With the DARPA database, including invasive, the detection rate for the ANN-based approaches proposed by Ghosh, A.K et al (1999), was found to be 77%, while the false positive rate was just 3%. False positives were eliminated by Ghosh et al. (1999) when they employed a different form of artificial neural network (ANN) to solve the same issue.

Lakhina, A., Crovella, M. and Diot, C. in 2005 suggested a network anomaly detection approach based on entropy measures and contrasted the findings obtained with a volume metric to see which was superior. As the article points out, network traffic feature distributions may be enhanced by the inclusion of additional information that can be utilised to identify network anomalies.

Using K-Means clustering, which is one of the most often utilised strategies, is simple and effective. For the identification of intrusions, Eslamnezhad, M. and Varjani, A.Y., in 2014 used a modified K-Means technique known as Min-Max K-Means. The suggested K-means method has an overall detection rate of 81%, compared to 75% for the traditional K-means algorithm. It also has a reduced false-positive rate than the traditional K-Means method.

There is an IDS developed by Manzoor, I. and Kumar, N., (2017) based on the ANN classifier that uses correlations to get its reduced set of features. For classification purposes, these correlations are utilised to rank characteristics in relation to the class and evaluate whether or not a feature is significant. According to results from the KDD Cup 99, the proposed technique exhibited an enhanced model accuracy and decreased false alarm rate after the training and testing procedures.

To categorise assaults in the UNSW-NB15 dataset, Yang, S.U., 2019 employed a bidirectional LSTM based technique. Recurrent neural networks, of which an LSTM is a subset, are known as LSTMs. Class imbalance in the UNSW-NB15 dataset affected the LSTM IDS's ability to identify malicious activity, but its overall performance was not affected. Next, the writers decided to focus on resolving the issue of class imbalance.

All the above research used pre-existing databases or datasets on which they performed analysis and gave results that are not applicable to the real world. The research paper's author simulated the real-time conditions for detection of intruders in real time.

RESEARCH APPROACH

In this research the intelligent system in introduced to detect the probe attacks from the intruders. This research is the combination on machine learning and cyber security. Artificial neural network is used to detect the attacks in the testbed network by training on the data. For this experiment the researcher collect the data from the testbed, pre-processed it and trained the neural network.

The data is collected from the experiment setup by the researchers. This setup consists of 2 attackers with different operating systems using windows and ubuntu known as pc-test2 and pc-test4. Both the attackers have spoofed their mac configuration using the software. The genuine user is known as pc-test1, who is using the network for various tasks. The pc-test3 is the monitor pc which uses a tool called Wireshark for capturing the data on the wifi router (Ratnayake, D.N., et al,2011). This data consists of various frames and information.

The pre-processing task is done when the pc-test3 captures the data. The data captured by the wireshark has lot of variables but for this experiment only delta time value, sequence number, received signal strength, and frame sub-type of the packets transmitted are used and the other data is removed.

The training is done by using ANN which uses Levenberg-Marquardt back propagation. The network consists of 4 inputs, one hidden layer with 20 neurons and one output layer which single output. The tanh activation function is used in all the layers.

After training on 70% of the total dataset and 15% of the validation dataset, the model was detecting 99% to 100% for known attacks and giving accuracy of 89% for unknown attacks in the test set (Ratnayake, D.N., et al,2011).

The pro of this research is that it was able to develop and training a neural network which was replicating the real-world scenario. The research also was the detection rate when the user and attackers are moving the in room which is good as in real life the person is not standing at one place.

The con of this research is that it is using simple neural network of the prediction. I think it is better to implement a RNN like LSTM which can store data in the network as memory and use that memory to detect the intruders.

PERSONAL INVESTMENT

I think the research gap found by the researcher was quite significant. As this is the known security flaw till date even after many iterations of wifi standards. I think intelligent systems needs to be developed to protect the users and make the resource available to the genuine user.

I have worked with DARPA dataset for intrusion detection using ANN. That was my assignment during my computer science degree. Due to that project I have gained quite a good amount of knowledge about the intrusion detection techniques.

REFERENCE:

Eslamnezhad, M. and Varjani, A.Y., 2014, September. Intrusion detection based on MinMax K-means clustering. In 7'th International Symposium on Telecommunications (IST'2014) (pp. 804-808). IEEE.

Geetha, K. and Sreenath, N., 2014, February. SYN flooding attack—Identification and analysis. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-7). IEEE.

Ghosh, A.K., Schwartzbard, A. and Schatz, M., 1999, April. Learning Program Behavior Profiles for Intrusion Detection. In Workshop on Intrusion Detection and Network Monitoring (Vol. 51462, pp. 1-13).

Guo, F. and Chiueh, T.C., 2005, September. Sequence number-based MAC address spoof detection. In International Workshop on Recent Advances in Intrusion Detection (pp. 309-329). Springer, Berlin, Heidelberg.

Lakhina, A., Crovella, M. and Diot, C., 2005. Mining anomalies using traffic feature distributions. ACM SIGCOMM computer communication review, 35(4), pp.217-228.

Manzoor, I. and Kumar, N., 2017. A feature reduced intrusion detection system using ANN classifier. Expert Systems with Applications, 88, pp.249-257.

Ratnayake, D.N., Kazemian, H.B., Yusuf, S.A. and Abdullah, A.B., 2011. An intelligent approach to detect probe request attacks in IEEE 802.11 networks. In

Engineering Applications of Neural Networks (pp. 372-381). Springer, Berlin, Heidelberg.

Robinson, F., 2004. 802.11 i and WPA Up Close. NETWORK COMPUTING-MANHASSET NY-, 15(6), pp.79-82.

Tippenhauer, N.O., Rasmussen, K.B., Pöpper, C. and Čapkun, S., 2009, June. Attacks on public WLAN-based positioning systems. In Proceedings of the 7th international conference on Mobile systems, applications, and services (pp. 29-40).

Yang, S.U., 2019, March. Research on network behavior anomaly analysis based on bidirectional LSTM. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 798-802). IEEE.

PART 2: ARTIFICIAL INTELLIGENCE SPECIALISM.

INTRODUCTION

Commercially accessible home robots with human-like interaction characteristics tend to be used for entertainment purposes rather than for practical purposes. Robots in the future will have to meet two primary conditions if they are to find a more beneficial role in a human-oriented residential environment (Rezazadegan, F.,et al,2015) :

System's technological capabilities: You need it to be versatile so that you may use it for many different purposes.

Social capabilities: These activities or functions need socially acceptable, pleasant, and effective methods of carrying them out for the people with whom it shares the environment and interacts.

To perform valuable activities in an environment where humans are present, a robot's technological skills must be thoroughly researched by numerous scientists, who are now working on this issue. It’s possible that the second criteria are just as significant, since if the robot exhibits behaviours that aren't considered socially acceptable, people may reject the robot out of hand. There is a fast-growing discipline called Human-Robot Interaction that studies socially interactive robots and gives a taxonomy of design methodologies and system components (Saenz, J.,et al,2018) . Human-Robot Interaction is one such quickly increasing topic that include research into social robots.

OPEN RESEARCH QUESTIONS

This research is focused on interlinking social abilities of the robot and safety engineering of the robot which is a technical aspect. The artificial intelligence specialism discusses about “what is the link between an assistive robot’s social credibility and its effective safety performance?”

The physical appearance of a domestic service robot will be distinct from that of a computer or most other household items since it will be mobile. As the robot does its duties, it will encounter humans and will need to use socially appropriate verbal and nonverbal cues to avoid making people uncomfortable or irritated in their own house. This is the real-world problem where many researchers are facing problems to solve it. Safety and societal problems are increasingly being taken into account while developing assistive robots. As a result, the robots are designed to be safe and socially acceptable to humans. Requirements to ensure the safety of the robot might have a negative influence on the robot's ability to interact with humans (Hancock, P.A.,et la,2011). It's possible that the safety requirements for robots, and the behaviours necessary to achieve them, may be overlooked in the process of developing social behaviour. Specifically, this research topic covers the issues.

For the real-world application, we can link the research to people who are suffering from dementia. People with dementia are unstable and constantly in a mood of panic. If the assistive robot is taking care of a person by helping them with their daily activities and reminding them of their medication, etc., It needs to approach them in a human-like manner so that they feel comfortable and safe. This application requires the robot to perform tasks safely and in a socially acceptable manner. By encouraging and promoting nonverbal communication throughout the therapeutic encounter, Marti, P., Giusti, L. and Bacigalupo, M., (2008) supported a non-pharmacological therapy for dementia that emphasises social context, motivation, and involvement. A novel adaptive socially assistive robotic (SAR) system, on the other hand, is proposed in this paper in order to give a tailored protocol for users who are experiencing cognitive changes as a result of ageing or Alzheimer's disease.

RELATED WORK

Surveys of human action learning and human-robot cooperation were sparked by the development of learning algorithms. Hand gestures, facial expressions, and body movements were often used to describe behaviour in the texts cited. " According to Thomaz, A et al (2016) , the HRI programme may be used to analyse human emotions and activities via verbal and nonverbal expressions and actions. They also spoke about human-robot cooperation and robot imitations of human social behaviour in encounters. Nonverbal expressions of agreement and disagreement were the topic of a study by Bousmalis et al (2011) , which examined how these expressions are represented and detected. An overview of attention detection and its applications in social robot platforms was presented by Ferreira et al. As part of their study on human-robot interactions, they discovered that attention had a significant impact on the outcomes of such encounters.

There is an ongoing debate over how to ensure the safety of robotic systems, which was examined in a recent study by Boddington. P (2017). Safety in robots, according to EPSRC guidelines, encompasses not only physical but also psychological, social, moral, and other vital aspects.

Experiments by Joosse, M.,et al (2014) show that an agent's approach speed varies with the degree of penetration in personal space, based on their proxemics hypothesis. The extent to which robots adhered to these social rules had a profound effect on humans. For the purpose of improving the robot's motion planner, Feil-Seifer, D. and Matarić, M., (2011) utilised human examples to create a model of optimal following behaviour. To construct robot response behavioural models for various situations in ADL tasks, the researchers in Kostavelis, I et al. (2017) drew on surveys done on individuals with early Alzheimer's disease. POMDPs were used to establish a probabilistic interaction policy that governed the robot's behaviour depending on the chosen robot actions in order to solve a scenario. Observations of sensor congestion were partially compensated for while the most relevant robotic intervention actions were determined. The incentive function was therefore regulated by altering robot alert levels in relation to user condition.

Most of the already present work focused on particular group of people with any disabilities and the research was done. this type of research is not applicable for the whole population and regular people can get annoyed by the robot which learnt to behave with a particular group of people. But the research which is done is not based on particular group but is more focused on improve the social behaviour of the robot.

RESEARCH APPROACH

The experiment study was conducted on 30 participants in the robot house, which is equipped with various sensors and devices. The experiment was conducted by manipulating the behaviour of the robot while communicating with the participants. Half of the participants were involved with polite robots with social norms, and the other half of the participants interacted with unpolite robots that violated social norms (Holthaus, P.,et al 2019). These social standards were established through the robots' actions, such as greeting, moving the robot, and interpreting location and communication mode.

In the experiment, the participants sit on the table and solve the puzzle. The participants are interrupted by the robot for a safety alert. The researchers installed three alerts that, when activated by the robot, will notify the participant. These hazards consist of the oven being switched on, plugs being turned on, and the overheating of the pepper robot (Holthaus, P.,et al 2019). These alerts are classified into 3 categories: severe, moderate, and minor. Both of them become independent variables with the researcher changing to see the effect on the behaviour of the participants.

The behaviour of the participants is measured by the actions taken by them and their perception of the robot's behaviour. The measure is calculated by the questionnaire, which was conducted after the experiment. The degree of each danger was estimated using a semantic questionnaire, which was used in the data collection process. The RoSAS and Godspeed questionnaires were used to examine the participant's assessment of the robot's social behaviour. In order to find out whether they are really interested in reacting to robot warnings, open questions are employed (Holthaus, P.,et al 2019).

The results show that people in the polite condition tended to pay more attention to the robot's danger warnings, particularly during the second plug phase. In addition, the response rate has dropped significantly after the initial warning about power plugs. When participants displayed a response in the polite condition, they nearly always took action, but in the unpolite condition, they occasionally responded but opted not to manipulate things (Holthaus, P.,et al 2019).

The advantage of the research is that it took the right step towards integration of robot parts into humans' lives and tried to bring robots close to human social behaviour.

The drawback of the experiment is that a participant only knows the polite or unpolite part of the experiment, which can be effective. If a participant has interacted with both kinds, then we can measure the change in attitude of the participants, which is more helpful in designing a robot.

PERSONAL INVESTMENT

I think the research gap found by the researcher was quite significant. In the future, robots must be built with social and technical aspects in mind. This research tried to bring both the aspects together and gave early evidence of a link between social trustworthiness and social robots' safety authority.

As a data science student, I would like to learn and improve the technical aspects of the robot and improve the efficiency of doing work.

REFERENCE:

Boddington, P., 2017. Towards a code of ethics for artificial intelligence (pp. 27-37). Cham: Springer.

Bousmalis, K., Morency, L.P. and Pantic, M., 2011, March. Modeling hidden dynamics of multimodal cues for spontaneous agreement and disagreement recognition. In 2011 IEEE International Conference on Automatic Face & Gesture Recognition (FG) (pp. 746-752). IEEE.

Feil-Seifer, D. and Matarić, M., 2011, August. People-aware navigation for goal-oriented behavior involving a human partner. In 2011 IEEE International Conference on Development and Learning (ICDL) (Vol. 2, pp. 1-6). IEEE.

Hancock, P.A., Billings, D.R., Schaefer, K.E., Chen, J.Y., De Visser, E.J. and Parasuraman, R., 2011. A meta-analysis of factors affecting trust in human-robot interaction. Human factors, 53(5), pp.517-527.

Holthaus, P., Menon, C. and Amirabdollahian, F., 2019, November. How a robot's social credibility affects safety performance. In International Conference on Social Robotics (pp. 740-749). Springer, Cham.

Joosse, M., Sardar, A., Lohse, M. and Evers, V., 2013. BEHAVE-II: The revised set of measures to assess users' attitudinal and behavioral responses to a social robot. International journal of social robotics, 5(3), pp.379-388.

Kostavelis, I., Giakoumis, D., Malassiotis, S. and Tzovaras, D., 2017, July. A pomdp design framework for decision making in assistive robots. In International Conference on Human-Computer Interaction (pp. 467-479). Springer, Cham.

Marti, P., Giusti, L. and Bacigalupo, M., 2008. Dialogues beyond words. Interaction Studies.

Rezazadegan, F., Gengb, J., Ghirardi, M., Menga, G., Murèb, S., Camuncolib, G. and Demichelac, M., 2015. Risked-based design for the physical human-robot interaction (pHRI): An overview. Chemical Engineering Transactions, 43, pp.1249-1254.

Saenz, J., Elkmann, N., Gibaru, O. and Neto, P., 2018, February. Survey of methods for design of collaborative robotics applications-why safety is a barrier to more widespread robotics uptake. In Proceedings of the 2018 4th International Conference on Mechatronics and Robotics Engineering (pp. 95-101).

Thomaz, A., Hoffman, G. and Cakmak, M., 2016. Computational human-robot interaction. Foundations and Trends in Robotics, 4(2-3), pp.105-223.