DETECTING THE INRUSION IN THE PERVASIVE ENVIRONMENT USING COMBINED LEARNING APPROACH

A.KRISANTHA[#1] M.KALIMUTHU[*2]

[#]*DEPARTMENT OF COMPUTER AND COMMUNICATION*

SNS COLLEGE OF TECHNOLOGY, VAZHLIYAMPALAM,

SARAVANAMPATTI,COIMBATORE-35,INDIA.

[1]gabrielajerolin@gmail.com

**SNS COLLEGE OF TECHNOLOGY, VAZHLIYAMPALAYAM*

SARAVANAMPATTI, COIMBATORE-35, INDIA.

[2]mkmuthu73@gmail.com

Abstract-- Nowadays detection of the passive intrusion in an pervasive environment witnessed an special interest ,e.g., protection for the people in the emergency time and also for the industrial purposes. Most of the past studies focused on a single intrusion pattern with moving variance captured using indicators at a time. In the day today life, any number of the intrusion pattern can be detected by combining indicators together. Thus the combined learning approach of many indicators effectively indicates the presence of intrusions. The performance of the detection technique enhances the detection with many transmitter and receiver pairs and provide efficiency of the approach nearing to the zero false positive rate.

I.Introduction

Wireless communication systems creates chances to change the computing methods in pervasive environments. The environmental changes up to the density of an wireless networks and equipped with sensing capabilities . Wireless infrastructure is mainly used for the communication , and the wireless sensing data is dual-used for the intrusion detection in wireless environments. In the day today life there is an increasing availability of pervasive wireless infrastructure in the industries, office buildings, transportation infrastructure, and military battlefields. These pervasive wireless infrastructure is used in a broad array of applications such as , intrusion detection in industries for asset protection, notifying the trapped people in a fire building during emergency , and battlefield security.

The Signal Strength obtained from the wireless infrastructure for performing intrusion detection when the intruders or objects do not have any radio devices attached to them. This is also known as passive intrusion detection [1].Most of the existing intrusion detection techniques utilizes mainly the video, pressure, infrared, pre-deployment of specialized hardware, and not easily deployed for unscheduled tasks and may not be scalable. Wireless localization schemes consist of existing wireless infrastructure to perform localization, these schemes require the particular object to carry a radio device or actively participating localization.

Detecting and localizing intrusion objects that either requires specialized infrastructure setup that relies on communication devices attached to objects, an alternative method on device-free passive wireless localization [8] has shown the feasibility of using radio signal dynamics for object detection in wireless environments which detects intrusion events in a controlled environment. It has the ability in capturing one intrusion pattern when the intruders are moving around. They cannot detect the type of events when the intruders are static in nature. For instance, an intruder is standing alone and hiding somewhere, or a person is trapped in a fire building.

In our real-world, there are many intrusion patterns such as standing alone, hiding somewhere, and moving in a paticular direction, which is detectable by employing the detection power of different intrusion indicators combined and has the ability in combining the detection power of intrusion indicators enhancing the performance of intrusion detection.

B. Works and Intrusion Learning

Various technologies are used to detect intruders in various environments including corporate, civilian, and military. They all are actively working with the use of video, pressure, ultrasound and infrared. [2] utilized video is used to analyze sequences of images captured by cameras and to track the moving people. The video-based one is very expensive, label intensive and also it fails in dark environments. The people who are being tracked in this mainly raise privacy concerns [3]. deployment of the air pressure sensors under the floor to detect the footsteps of people and build an profile based on the footsteps of people, and ultra vision [9] produces ultra-sensor motion detection sensors. Deploying sensors causes high cost, and low scalablity.

The methods which are relying on ultrasonic Time-of-Arrival and on the Time-Difference-of-Arrival between ultrasound and RF signal performs both static and mobile object localization. The network using ultrasound conducts the localization and possible object tracking which require specialized infrastructure, and each particular object carries a wireless device which uses an infrared infrastructure to achieve localization estimation. However, the infrared technology also needs a specialized infrastructure, having a short range and dense deployment. This technique can be further classified based on ranging methodology. Range based method involve distance estimation to access points using the measurement of various physical properties. The range-free method [14] uses coarser metrics to place bounds on candidate positions. All of these schemes requires the paticular object to carry a radio device and active participation in localization.

In these products usually specific chip sets and operating systems are required. The device-free is a new concept to localize and track paticular objects without carrying radio devices and actively participate in the localization process, which use the signal dynamic property between the static environment and the dynamic environment to conduct transceiver-free object tracking in wireless sensor networks[17] deployment of a Radio Tomographic Imaging system, which uses large number of wireless nodes to image passive objects within a wireless network. The works that are most closely related to combined learning [1] demonstrates the feasibility of device-free passive localization in a controlled environment using the moving average and the variance of signal strength, to detect the events and conducts localization based on passive radio map construction. Whereas [1] performed passive event detection in real environments using the moving variance and results in a low precision. Their detection capability is limited as single intrusion indicator . Combined learning approach is generic in nature and combines the detection power of intrusion indicators. And also it is highly flexible to incorporate new indicators, and consequently maximize the performance of passive intrusion detection. Passive intrusion detection based on the signal strength is the data collected in pervasive wireless environment which is especially attractive and reuses the existing wireless environmental data without requiring a specialized infrastructure such as surveillance camera based intrusion detection [18]. Under critical situations like emergency evacuation in a fire building, it is difficult to detect and locate people trapped inside the building in a timely manner.

Reusing the environmental sensing data, such as signal strength ,does not provide tremendous cost savings , the collected sensing data can be dual-used for intrusion learning, and it is available at any time for performing detection analysis. The specialized hardware infrastructure has already been installed for import protection, the wireless environmental data can assist to refine the process of intrusion detection. And also the radio signal is affected by reflection signal, refraction signal, shadowing signal and scattering signal, the strength of the signal at wireless devices are relatively stable if there is no movement or changes in wireless environments and it will get affected if there is a presence of intrusions, for an instance, the intruder is standing alone , walking in a wireless environment will absorb, reflect, and diffract some of the transmitted power.

At the same time, the signal strength at wireless devices gets impacted and results in change of signal strength values. Based on the change of signal strength at wireless devices ,intrusion devices is possible. Performing passive intrusion detection is an challenging method where the intruders usually do not carry any radios and are not cooperative. The main issue is that need to be addressed in order to make it feasible and to perform passive intrusion detection in wireless environment , collects the signal strength data which is affected by the noisy environment. filtering the measurement errors and clean up the noise to make it effective utilizing the different characteristics captured by intrusion patterns, the passive intrusion detection scheme should be able to effectively differentiate those intrusions based on different profiles. To address these issues, pattern profiling method and detection scheme based on combined learning is used.

3.) *Intrusion Learning Scheme and Methodology*

Intrusion detection strategy utilizing multi-pair collaboration on top of grid-based clustering. De-clustering Effect, The relationship between the mean of values and the variance of signal strength values when intrusions are present clustering effect under normal situations, whereas the presence of intrusions result in a de-clustering effect of points. It can also be said as,the points are more spread when there are standing or moving intruders. The presence of intrusions is obvious with the combining view of the mean and variance of the signal strength. Thus, we call the mean and variance of signal strength readings as intrusion indicators, which can be used to diagnose intrusion activities combined.

Grid-based Clustering To capture the de-clustering effect under intrusion, we use grid-based clustering which combines the detection power of different intrusion indicators to perform a combined learning of intrusions. Since a grid is an efficient way to organize a set of data points [21], breaks the d dimensional space of d different intrusion indicators into grid cells, performs clustering based on the density of data points in each grid cell. The objective combined approach is

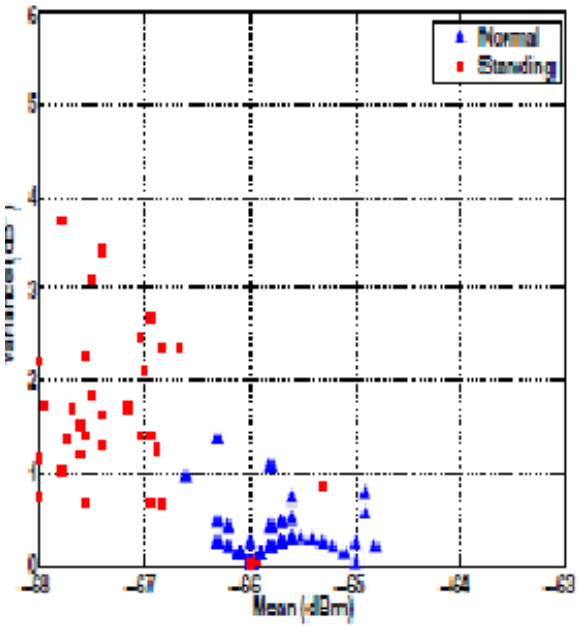

Fig.1 Normal and Standing

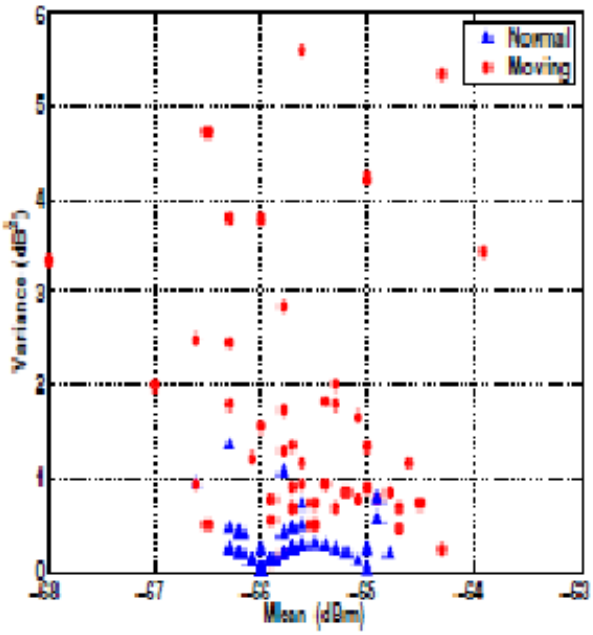

Fig.2 Normal and Moving

to capture the de-clustering effect by partitioning the data into two clusters so that one cluster has a higher density and the other has a lower density. Suppose there are d different intrusion indicators, which construct the d-dimensional data space S .Let D = {S1, S2, ..., Sn} be the input of data and Si ={si1, si2, ..., sid}, where sij is the value of the ith data point of the jth intrusion indicator. The method partitions the whole data space S into non-overlapping grids by partitioning each dimension into N equal length intervals. The intersection of one interval from each dimension forms one grid, which can be denoted by the form {g1, g2, ..., gd}

where gj = [rj, lj) is one interval of jth dimension. The data point Si falls into a grid if rj ≤ sij < lj for all j (i.e.j = 1, 2, ..., d). All data points are placed into grids based on this simple criteria .A grid is a core grid if the number of points fall into the grid exceeds the density threshold , which can be derived empirically. A grid is a border grid if the number of points falling into the grid is less than threshold . And the grid is within the core grid. In this study, we set K to 8. A grid p is directly reachable from a grid q if p belongs to q's K-neighborhood and q is a core grid. A grid p is reachable from a grid q if there exist some intermediate grids p1, p2, ..., pn, p1 = p, pn = q such that p(i+1) is directly reachable from pi. A grid p is connected to a grid q if there is a grid o such that both p and q are reachable from o or if p and p are all core grids and the distance between these two grids is less than the Manhattan distance . A grid cluster is a maximal set of connected grids. Finally, combined method partitions all the data points that fall into the grid cluster into a dense cluster and the rest of the points into a sparse cluster .indicators to illustrate how combined might operate. The two intrusion indicators we use to validate are: the average mean and the variance of signal strength. The density threshold and the distance based on our empirical study using data without intrusion events. The experimental data points have been partitioned into two clusters with different densities in In particular, the points from normal data without intrusion have been placed in the dense cluster ,whereas points of intrusion data have been placed in the sparse cluster The key observation here is that the cluster formulation by combined is consistent with the distribution of data points indicating that clustering based on grid density is feasible to capture intrusion effects.

Once the data points are partitioned into two clusters, will have significantly different density when there are intrusions present. In other words, when intrusions are present, the sparse cluster produced represents the points affected by intrusion, whereas the dense one representing points not affected by intrusion. To measure whether the density distributions of the two partitioned clusters are significantly different, we use statistical hypothesis testing is defined as:H0 : two clusters are statistically the same .A student t-test [22] on the two clusters obtained to calculate the p-value of the test statistic. The goal is to see whether the resulted p-value is less than the significant level. If the p-value is larger than the significant level, the null is accepted In particular, suppose the two clusters are C1 = {p1, p2, ..., pn} and C2 = {q1, q2, ..., qm}.Further, the distribution of the test statistic t is approximated as an ordinary Student's t distribution with the degrees of freedom calculated.

From the value of the test statistic t and the degrees of freedom, we obtain the p-value from the student's t distribution. By comparing p-value with the significant level, the output can be made on whether to accept the null or not .If the p-value is less than the given significant level, indicating that the density distributions of the two clusters are different from each other, when the null is rejected the presence of intrusions is declared. Multi-pair Collaboration, intrusion detection relying on the data from only one

transmitter-receiver pair may provide weak evidence of the presence of intrusions and trigger a false positive As wireless networks become more pervasive, the wireless devices can be deployed with sufficient density such that the same intrusion event can be observed from the data collected from multiple transmitter receiver pairs. Thus, to reduce false positive and increase the detection accuracy, using the observations from multiple transmitter-receiver pairs to collaboratively determine the presence of intrusions. Integrating multi-pair collaboration enhances the reliability of intrusion detection, mainly in noisy environments .In multi-pair collaborative learning, an alert when one transmitter-receiver pair has p-value below the significant level. The presence of intrusions when the number of alerts among all available transmitter-receiver pairs during one examining time period exceeds the learning threshold. The learning threshold in our strategy is adjustable based on the total number of available transmitter-receiver pairs in the area of interest.

By examining the t-test results of static events indicates that the partitioned two clusters have significantly different distributions and there are intrusions present in the wireless environments .under normal conditions, the p-values are much larger than the significant level, indicating that the partitioned two clusters do not have significant difference, and thus there is no intrusion present in the system. Similar observations for moving events where most of the p-values are much lower than the significant level when experiments are walking around in the experimental area. These results are encouraging as they indicate that our detection strategy based on hypothesis testing using t-test is feasible in diagnosing the presence of intrusions.

Found that p-values of certain transmitter-receiver pairs are above the significant level when intrusions are present. This may be due to signal interference or random noise in the environment, which causes these transmitter-receiver pairs failed to observe the presence of intrusion. However, the presence of the intrusion can still be detected by using the multi-pair collaborative strategy in combined learning scheme. By using the multi-pair collaborative approach, we evaluate the p-values of all the transmission-receiver pairs in the same examination time period and report the detection of intrusion when at least one pair has p-value less than the significant level. That is, even when some transmitter-receiver pairs failed to observe the presence of intrusions, other pairs in the close-by neighborhood can complement the detection function, and consequently maximize the detection power .Performing passive intrusion learning accurately is challenging as to differentiate an intentional intrusions scenario from noisy environments. Handled properly, the disturbance caused by noises would easily trigger false detection. Thus, for a scheme to be effective for passive intrusion learning, it is crucial to minimize the false positive rate, while achieving high detection rate .Study the effectiveness of our multi-pair collaborative strategy in terms of false positive rate and the corresponding intrusion detection rate.

Observed that when increasing the number of alerts, which work collaboratively to determine the presence of intrusions, the false positive rate goes down to 0% quickly with2 alerts the detection rate is about 89% when the number of alerts is set to 2 and 3,the detection rate keeps at 100% when the number of alerts ranges from 1 to 7. Comparing to [1], which resulted in a low precision of about 0.3, our approach achieves a much higher precision by performing combined learning. In particular, the precision is 0.9 when alerts is 2 and 3 in the key observation here is that using multi-pair collaborative detection can significantly reduce the false positive rate, while keeping high detection rate, indicating that detection using multiple transmitter-receiver pairs is highly effective in differentiating intentional intrusions from random environmental changes.

Impact of Device Density examine the impact of wireless device density on the performance of our detection scheme This indicates that when intrusion is present in the area of interest, there are potentially more wireless devices . Consequently, when diagnosing the presence of intrusions, there are more wireless devices that can work together to perform intrusion detection collaboratively . Our multi-pair collaborative strategy also brings another dimension of knowledge of identifying problematic wireless devices. For instance, we observed that the transmitter-receiver pair has high p-values, which is different from its neighboring pairs, indicating that the wireless devices are not reliable during data collection and may have hardware deficiencies. work will further quantify the relationship between the detection power and the density of wireless density.

.Differentiating Intrusion Events Detecting the presence of intrusions in the system provides first order information towards defending against them. Learning the different intrusion patterns allows the system to further determine the appropriate defense strategies in the next step. Differentiating the intruder which is hiding in a place or moving around will enable the next step of action to either capture the intruder or follow him; or learning a person is trapped in a fire building will allow the fire fighters to determine the best rescue strategy.

Observed that the moving intrusion instances tend to produce in larger variance of signal strength when compared with the static intrusion instances. This suggests that it is feasible to use the moving variance to differentiate intrusion patterns in passive intrusion detection .For each transmitter-receiver pair, moving variance during the examining time period for each pair is the accumulated results by adding up the averaged moving variance from each pair. The values of variance of static events are much smaller than those of moving events. This is because intruders moving around cause changes in wireless environments constantly, which results in higher value of variance. Therefore, by using accumulated moving variance in combined learning scheme, effectively differentiate intrusion patterns.

IV. CONCLUSIONS

To perform combined learning for detecting intrusion when intruders do not carry any wireless devices .Our combined learning approach combines the detection power of complementary intrusion indicators and has the capability to detect different intrusion events in wireless environments. In particular, utilizes the Signal Strength from the existing wireless infrastructure and exploited to use the changes of signal strength caused by intrusions for diagnosing the presence of intrusions. Profiled environmental uncertainties through data cleansing and intrusion pattern derivation. Which captures the de- clustering effect in intrusion indicators when intrusions are present. Additionally, our detection strategy utilizing multi-pair collaboration can enhance the reliability of intrusion detection under noisy environments.

The performance of our combined intrusion learning approach using false positive rate and detection rate. Experimental results provide strong evidence of the feasibility of performing joint learning for passive intrusion detection .our strategy of using collaborative efforts across multiple transmitter-receiver pairs can complement the detection function and maximize the detection power nearing to the zero false positive rate . Finally, an interesting observation is that the collaborative detection strategy can also bring another dimension of knowledge of identifying problematic wireless devices, which report wrong signal readings

REFERENCES

[1] M. Moussa and M. Youssef, "Smart devices for smart environments :Device-free passive detection in real environments," in The 2nd IEEE Workshop on Intelligent Pervasive Devices, March 2009.

[2] Q. Cai and J. K. Aggarwal, "Automatic tracking of human motion in indoor scenes across multiple synchronized video streams," in Proceedings of the Sixth International Conference on Computer Vision, 1998.

[3] J. O. Robert and D. A. Gregory, "The smart floor: a mechanism for natural user identification and tracking," in Proceedings of the CHI 200 Conference on Human Factors in Computing Systems, 2000.

[4] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2000, pp. 775–784.

[5] E. Elnahrawy, X. Li, and R. P. Martin, "The limits of localization using signal strength: A comparative study," in Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004), Oct. 2004, pp. 406–414.

[6] P. Enge and P. Misra, Global Positioning System: Signals, Measurementsand Performance. Ganga-Jamuna Pr, 2001.

[7] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricketlocation-support system," in Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), Aug 2000, pp. 32–43.

[8] M. Youssef, M. Mah, and A. Agrawala, "Challenges: Device-free passive localization for wireless environments," in Proceedings of the ACM International Conference on Mobile Computing and Networking(MobiCom), Aug 2007.

[9] "Ultravision Corporation," white paper available at http://www.ultravisionsecruity.com.

[10] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," ACM Transactions on Information Systems, vol. 10, no. 1, pp. 91–102, Jan. 1992.

[11] K. Kleisouris, Y. Chen, J. Yang, and R. P. Martin, "The impact of using multiple antennas on wireless localization," in Proceedings of the Fifth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2008.

[12] J. Yang and Y. Chen, "A theoretical analysis of wireless localization using RF-based fingerprint matching," in Proceedings of the Fourth International Workshop on System Management Techniques, Processes, and Services (SMTPS), April 2008.

[13] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005), 2005, pp. 91–98.

[14] T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes in large scale sensor networks," in Proceedings of the Ninth Annual ACM International Conference on Mobile Computing and Networking (MobiCom'03), 2003.

[15] "Airtight networks," white paper available at http://www.airtightnetworks.net.

[16] D. Zhang, J. Ma, Q. Chen, and L. M. Ni, "An rf-based system for tracking transceiver-free objects," in Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2007

[17] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," in Tech Report, Sep. 2008.

[18] D. B. Yang, H. H. Gonzalez-Banos, and L. J. Guibas, "Countingpeople in crowds with a real-time network of simple image sensors," in Proceedings of the Ninth IEEE International Conference on ComputeVision, 2003.

[19] J. Bednar and T. Watt, "Alpha-trimmed means and their relationship to median filters," Acoustics, Speech and Signal Processing, IEEE Transactions on, vol. 32, no. 1, pp. 145–153, Feb 1984.

[20] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, "A practical approach to landmark deployment for indoor localization," in Proceedings of the Third Annual IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks (SECON), Septembe 2006.

[21] P.-N. Tan, M. Steinbach, and V. Kumar, Introduction to Data Mining. Addison-Wesley, 2005.

[22] G. Casella and R. L. Berger, Statistical Inference. Belmont, California:Duxbury Press, 19

.

