International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Artificial Intelligence Based Intrusion Detection for Wireless Sensor Networks-A Review

Ashwani Kumar[1], Sumit kumar Gupta[2], Ankur shukla[3]
Electronics and Communication Engineering Department,
Bansal Institute of Engineering and Technology, Lucknow
samratashwani23@gmail.com

Abstract: Manufacturing industries, medical devices, the positioning of military drones and bombs, and wireless communications and wireless sensor networks (WSNs) all heavily rely on them. The security of wireless communications is a very important issue that must be addressed appropriately given the scope of WSN use. A Product Characterized Remote Sensor Organization (SDWSN) is acknowledged by mixing a Product Characterized Organization (SDN) model in a WSN. In this paper, the cryptography plans as well as the security dangers connected with SDWSNs are recognized and the Man-made reasoning (simulated intelligence) procedures used to distinguish interruptions in SDWSNs are introduced. It is shown that a two-level security model joining cryptography plans and computer based intelligence strategies can be utilized to battle vindictive assaults against SDWSNs.

Keywords: Anomaly detection, Machine learning, Deep abnormality detection, Energy saving

1. Introduction:

A Wireless Sensor Network (WSN) is an organization made out of circulated hubs that can perform information obtaining and remote interchanges [1], [2]. Because wireless communications are more susceptible to interception than wired communications, WSNs are more susceptible to malicious attacks like distributed denial of service (DDoS) [3, 4]. Since WSNs are utilized for basic undertakings, for example, estimation of temperature in thermal energy plants and estimation of water level in water treatment plants [5], [6], Disavowal of Administration and Disseminated Refusal of Administration assaults on WSNs can bring about appalling outcomes like plant closures and blasts. The plant closures can prompt brief lay-offs and a deficit in the spending plan of plant representatives.

A Product Characterized Remote Sensor Organization (SDWN) is another worldview created by consolidating the WSN model and the Product Characterized Organization (SDN) [7], [8]. In a SDN model, the sending system of organization bundles (information plane) and the directing system (control plane) are decoupled to improve on the design and the administration of the organization [4].

SDWSNs are utilized in a variety of settings, including university networks, data centers, manufacturing industries, military headquarters, and more [6, 9], respectively]. Considering that the information communicated between the hubs and the regulators of an organization can be delicate (Colleges) or even grouped (military central command), the security of SDWSNs is a functioning field of exploration [11], [12]. In this paper, the cryptography plans and the Computerized reasoning (artificial intelligence) strategies utilized in SDWSNs are introduced. The blend of cryptography plans and computer based intelligence procedures is introduced as a suitable answer for battling assaults against SDWSNs.

2. Related Work:

Assaults on SDWSNs can be isolated into three classes [13], specifically objective orientated, entertainer orientated and layeroriented assaults.

Attacks with a focus on the goal can be passive or active [14]. Detached assaults are acted in other to take information without upsetting the organization. To take over the network, active attacks are launched. Instances of dynamic assaults incorporate wormholes and the notorious WannaCry.

Entertainer arranged assaults can be inside or outside assaults [15]. Inside assaults comprise of infusing noxious hubs into the organization to take information. Outside assaults comprise of infusing a malignant programming into the organization and can bring about a Disavowal of Administration (DoS) for genuine hubs. Layer-oriented attacks attack the network's layers [16].

The symmetric cryptography is otherwise called Secret Key Cryptography (SKC). The same key is used for both encryption and decryption in the SKC [17, 18]. Due to its simplicity, the Advanced Encryption Standard (AES) is the symmetric cryptography algorithm that is utilized the most frequently in SDWSNs [19, 20]. In the SKC, the restricted data should be stacked on every hub of the organization before sending to guarantee that every hub will actually want to decode the correspondence. The most significant drawback of the SKC is that it is unsuitable for large-scale SDWSNs due to the requirement that the secret information be loaded on all network nodes. Other than this inconvenience (versatility), it ought to be noticed that the way that the restricted data should be stacked on all hubs of the organization comprises a security shortcoming that can be taken advantage of by aggressors since by focusing on and effectively compromising a solitary hub they could take the privileged intel of the organization and thus compromise the entire organization. To defeat these disservices, the Area Based Key plan (LBK) can be utilized

[21], [22] yet the operations should be carefully coordinated to guarantee that every hub is put at the ideal area [23]. Along these lines, the pre-dissemination of irregular keys to every hub of the organization and the utilization of a believed base station can be embraced [24], [25]. It is important to note that if an attack on the network is successful using a pre-distributed keys scheme, an increase in the number of affected links will result from an increase in the number of captured nodes. The biggest drawback of using a pre-distributed keys scheme is this fact.

Public Key Cryptography (PKC) is another name for asymmetric cryptography. In the PKC, different keys are utilized for encryption and unscrambling [20]. The RSA calculation [26] and the Elliptic-Bend Cryptography (ECC) calculation are the most well known variations of the PKC [11], [27]. The chance of utilizing key understanding calculations or a key circulation plans in a PKC disposes of the need of utilizing the pre-dispersion of keys to every hub of the organization before the sending. This reality is the chief benefit of the PKC over the SKC. It ought to be noticed that the PKC presents the disservice of being more energy-serious than the SKC [12], [28].

The hybrid encryption offers both the efficiency of a SKC and the ease of use of a PKC [29]. It ought to be noticed that the half and half encryption is seldom utilized in SDWSNs since the SDWSN is another worldview and the mixture encryption is perplexing to execute.

There are two sorts of interruption location frameworks, in particular mark based discovery frameworks, and irregularity based interruption frameworks [30], [31]. In a mark based identification framework, new information are faced to a data set of recorded interruptions and the countermeasure framework is enacted when there is a match between the data set and new information. In an irregularity based interruption recognition framework, the ways of behaving of new information are checked to group them as typical or not typical (i.e., interruptions) [6]. It ought to be noticed that the mark based recognition frameworks neglect to recognize interruptions not kept in that frame of mind while the oddity based identification frameworks can identify zero-day interruptions.

Three classifications of artificial intelligence methods can be utilized to screen the security in SDWSNs to recognize interruptions [32], [33]. The primary classification incorporates conventional regulated learning methods, for example, the help vector machine and the innocent Bayes classifier. K-means and K-nearest neighbors, two semi-supervised learning methods, fall into the second category, while the deep learning approach falls into the third [33, 34].

A. Customary Managed Learning Calculations Wang et al. [13] proposed a calculation in light of the Help Vector Machine (SVM) to recognize the expected dangers to the organization. The SVM is a managed calculation utilized in man-made brainpower for order. As opposed to the calculated relapse, this calculation can make a non-straight choice limit between the components to be grouped and consequently can be applied to extremely confounded characterization issues [35]. Along these lines, Guileless Bayes (NB) classifiers can be utilized for grouping of correspondences between the regulators and the hubs of the organization. The peculiarity in rush hour gridlock streams can be utilized as a heuristic for anticipating on the off chance that an association or a hub introduced a danger to the organization. SVM and NB classifiers are suitable for preventing Distributed Denial of Service (DDoS) attacks in SDWSNs, but they are unable to adapt to new data.

Four semi-directed AI strategies can be utilized to shield an organization from noxious interruptions to be specific, the K-closest neighbors, K-implies, K-medoids and semisupervised innocent Bayes [36]. Barki and others 37] proposed a twolevel model for safeguarding a SDN against DDoS assaults. The primary level goes about as an inconsistency locator and decides whether a host is a potential danger given its way of behaving. The subsequent level goes about as an honesty checker and confirm in the event that the information communicated by the host are tainted. The previously mentioned AI calculations were to be utilized in the principal level of this model. The downside of semi-directed AI methods is their trouble to deal with a lot of information.

Profound learning are artificial intelligence methods that have significantly worked on the best in class in PC vision, text mining

what's more, speaker acknowledgment [38], [39]. Deep learning techniques can produce an accuracy of 90% in computer vision, whereas other AI methods can produce an accuracy of 75% [40, 41]. Thus, profound learning techniques are regularly utilized for undertakings like picture identification, object acknowledgment and picture division. A stream based interruption recognition framework (IDS) can utilize a multi-facet perceptron for identifying peculiarities [33], [42]. A multi-facet perceptron made out of an info layer, three secret layers and one result layer has shown to be serious with others approaches utilized for interruption identification in SDNs [33] when prepared on the NSL-KDD 1999 dataset [43]. The multi-facet perceptron accomplished a precision of 77.41 % on the test set while the best strategy (NB tree) accomplished an exactness of 82.02 % on the test set. The information layer of the multi-facet perceptron had the option to deal with six preselected elements of every bundle (i.e., input aspect was six) and the result layer has a component of two. The primary secret layer contained twelve neurons and each resulting stowed away layer contained the portion of the quantity of neurons of the past secret layer. On the NSL-KDD 1999 dataset, the accuracy of the NB Tree, the SVM, and the Deep Learning (Multilayer perceptron) [33] is shown in table II. The NB Tree strategy yields the most noteworthy precision (82.02%) while the SVM has the least exactness (69.52%). The multilayer perceptron method of deep learning has an accuracy of 77.41 percent. The exactness of the multi-facet perceptron can be expanded by adding more layers to the brain organization or preparing the multi-facet perceptron on a greater dataset [44].

A two-level security model can be utilized to safeguard SDWSNs against assaults [37], [45]. The principal level is the encryption of the correspondence between the hubs and the regulators of the SDWSN. It ought to be noticed that the three encryptions calculations (SKC, PKC and half and half) can be utilized from little to huge scope SDWSNs however every encryption strategy is more adjusted to a given scale due its innate disadvantages such versatility and energy utilization. The encryption calculation ought to be picked as per the size of the SDWSN, the correspondence speed required in the SDWSN and the energy utilization. For little SDWSNs, the SKC calculation ought to be leaned toward while for huge SDWSNs the PKC calculation ought to be liked. On the off chance that The speed and the security of the correspondence are considered to be basic for a given SDWSN, the cross breed encryption ought to be utilized.

The second level of the security model is the mix of an irregularity based IDS in the SDWSN. The streams between the hubs and the regulators of the SDWSN are investigated to recognize likely abnormalities. Prior to sending any bundle between a regulator and a hub of the SDWSN, the location of the hub is really taken a look at in a boycott. If the node's address is on the blacklist, the connection is cut; otherwise, the anomaly-based IDS looks to see if the packet has unusual behavior. Assuming the bundle presents peculiar ways of behaving, the hub is boycotted. The bundle is sent in the event that it doesn't present atypical ways of behaving.

3. Conclusion:

The security of SDWSNs against assaults can be accomplished by consolidating cryptography plans and computer based intelligence procedures for the counteraction and the identification of interruptions separately. The usage of man-made intelligence for safeguarding SDWSNs against interruption is as yet an open field of exploration since the SDWSN worldview has been as of late made. Deep learning and conventional algorithms like the SVM and the Naive Bayes are two AI techniques that could be utilized to guarantee that the security of a SDWSN is not compromised. These techniques have a few disadvantages like the need of a lot of preparing information, the flexibility to new information and the trouble of dealing with new information. These downsides should be addressed to acknowledge secure SDWSNs.

References:

[1] E. U. Ogbodo, D. Dorrell, and A. M. Abu-Mahfouz, "Cognitive Radio Based Sensor Network in Smart Grid: Architectures, Applications and Communication Technologies," IEEE Access, vol. 5, pp. 19084-19098, 2017.

[2] A. M. Abu-Mahfouz and G. P. Hancke, "Localised information fusion techniques for location discovery in wireless sensor networks," International Journal of Sensor Networks, 21_Publication in refereed journal vol. 26, no. 1, pp. 12-25, 2018.

[3] A. M. Abu-Mahfouz and G. P. Hancke, "Evaluating ALWadHA for providing secure localisation for wireless sensor networks," in 2013 Africon, 2013, pp. 1-5.

[4] S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz, "Security in software-defined wireless sensor networks: Threats, challenges and potential solutions," in 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), 2017, pp. 168-173.

[5] N. Ntuli and A. Abu-Mahfouz, "A Simple Security Architecture for Smart Water Management System," Procedia Computer Science, vol. 83, pp. 1164-1169, Jan 2016.

[6] D. Ramotsoela, A. Abu-Mahfouz, and G. P. Hancke, A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study. 2018, p. 2491.

[7] H. I. Kobo, G. P. Hancke, and A. M. Abu-Mahfouz, "Towards a distributed control system for software defined Wireless Sensor Networks," in IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 6125-6130.

[8] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "Fragmentation-based Distributed Control System for Software Defined Wireless Sensor Networks," IEEE Transactions on Industrial Informatics, pp. 1-1, 2018.

[9] M. Ndiaye, P. G. Hancke, and M. A. Abu-Mahfouz, "Software Defined Networking for Improved Wireless Sensor Network Management: A Survey," Sensors, vol. 17, no. 5, 2017.

[10] T. Azzabi, H. Farhat, and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," in 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), 2017, pp. 66-72.

[11] J. Louw, G. Niezen, T. D. Ramotsoela, and A. M. Abu-Mahfouz, "A key distribution scheme using elliptic curve cryptography in wireless sensor networks," in 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), 2016, pp. 1166- 1170.

[12] S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz, "Cryptography Methods for Software-Defined Wireless Sensor Networks," in 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), 2018, pp. 1257-1262.

[13] P. Wang, K. Chao, H. Lin, W. Lin, and C. Lo, "An Efficient Flow Control Approach for SDN-Based Network Threat Detection and Migration Using Support Vector Machine," in 2016 IEEE 13th International Conference on e-Business Engineering (ICEBE), 2016, pp. 56-63.

[14] P. H. Meland, E. Paja, E. A. Gjære, S. Paul, F. Dalpiaz, and P. Giorgini, "Threat Analysis in Goal-Oriented Security Requirements Modelling," in Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications: IGI Global, 2018, pp. 2025-2042.

[15] K. Shabana, N. Fida, F. Khan, S. R. Jan, and M. U. Rehman, "Security issues and attacks in Wireless Sensor Networks," International Journal of Advanced Research in

Computer Science and Electronics Engineering (IJARCSEE), vol. 5, no. 7, pp. pp: 81- 87, 2016.
[16] T.-G. Lupu, "Main types of attacks in wireless sensor networks," presented at the Proceedings of the 9th WSEAS international conference on signal, speech and image processing, and 9th WSEAS international conference on Multimedia, internet & video technologies, Budapest, Hungary, 2009.
[17] H. Ruotsalainen and S. Grebeniuk, "Towards Wireless Secret key Agreement with LoRa Physical Layer," presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 2018.
[18] T. Leighton and S. Micali, "Secret-Key Agreement without Public- Key Cryptography," Berlin, Heidelberg, 1994, pp. 456-479: Springer Berlin Heidelberg.
[19] S. K. Rao, D. Mahto, and D. A. Khan, "A Survey on Advanced Encryption Standard," International Journal of Science and Research, vol. 6, no. 1, pp. 711-724, 2017.
[20] W. Stallings, Cryptography and network security: principles and practice. Pearson Upper Saddle River, NJ, 2017.
[21] K. Sunil and D. Kamlesh, "Securing Mobile Ad Hoc Networks: Challenges and Solutions," International Journal of Handheld Computing Research (IJHCR), vol. 7, no. 1, pp. 26-76, 2016.
[22] Z. Yanchao, L. Wei, L. Wenjing, and F. Yuguang, "Securing sensor networks with location-based keys," in IEEE Wireless Communications and Networking Conference, vol. 4, pp. 1909- 1914, 2005.
[23] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in Proceedings of the World Congress on Engineering, 2015, vol. 1, pp. 1-3.
[24] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. Sen. Netw., vol. 2, no. 4, pp. 500-528, 2006.
[25] D. Wenliang, D. Jing, Y. S. Han, C. Shigang, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in IEEE INFOCOM 2004, 2004, vol. 1, pp. 1-597.
[26] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
[27] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, vol. 11, no. 4, pp. 2590-2601, 2017.
[28] A. Salomaa, Public-key cryptography. Springer Science & Business Media, 2013.
[29] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," Journal of Electrical Systems and Information Technology, vol. 2, no. 3, pp. 296-313, 2015.
[30] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, no. 1-2, pp. 18-28, 2009.
[31] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 255-264: ACM.
[32] O. G. Matlou and A. M. Abu-Mahfouz, "Utilising artificial intelligence in software defined wireless sensor network," in IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 6131-6136.
[33] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), 2016, pp. 258-263.
[34] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," presented at the Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, Hong Kong, China, 2013.
[35] S. Amari and S. Wu, "Improving support vector machine classifiers by modifying kernel functions," Neural Networks, vol. 12, no. 6, pp. 783-789, 1999.
[36] S. J. Russell and P. Norvig, Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited, 2016.
[37] L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," in 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 2576-2581.
[38] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," presented at the Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1, Lake Tahoe, Nevada, 2012.
[39] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, p. 436, 2015.
[40] A. Karpathy and L. Fei-Fei, "Deep visual-semantic alignments for generating image descriptions," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 3128-3137.
[41] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, Deep learning. MIT press Cambridge, 2016.
[42] Z. Jadidi, V. Muthukkumarasamy, E. Sithirasenan, and M. Sheikhan, "Flow-Based Anomaly Detection Using Neural Network Optimized with GSA Algorithm," in 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, 2013, pp. 76-81.
[43] (2018, August 10). KDD Dataset 1999 [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/
[44] A. Ng, "Machine Learning Yearning, 2016," ed: Stanford Press, 2017.

[45] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006.
[46] I. Goodfellow et al., "Generative adversarial nets," in Advances in neural information processing systems, 2014, pp. 2672-2680.