Intrusion Detection Mechanism To Mitigate Intrusion In MANET

IqraAbid, RanaMudassar Rasool , Muhammad Saleem, Muhammad Aleem, Riffat Hanif

Abstract ; Ad Hoc Network due to its infrastructure less ability. It has been providing lots of benefits in the field of communication and has changed the word into Global village. It has many features for example deployment facility, limited resources, dynamic topology and physical insecurity, the chances of attack increased than any other network. And due to dynamic topology, no static solution is applicable. There are two defense mechanism that can reduce the attack. First includes cryptography etc. If this defense is broken then intrusion detection system helps to reduce the attack ratio. In this survey paper, intrusion detection system taxonomy has been observed through different point of view. But the IDS detection mechanism has been elaborated in detail. And a comparison has been performed between the detection mechanism been used so far. Finally, we concluded useful information related to different mechanism and which mechanism has been used the most and performed well.

Keywords: MANET (Mobile Ad hoc Network), Intrusion, IDS (Intrusion Detection System), Mechanism, Wireless Network.

1. INTRODUCTION

In this era, where the world has changed into a global village due to the development of Technologies that helps in process of communication. Technology that are helping these days in better communication is network by helping to communicate between devices and the most important one type is the wireless network that makes communication possible between different devices without any wire or something to communicate between different people living in this world. The Internet of Things attracts due to its huge collection of applications and ease in real life, particularly for environments that are critical such as E-health, home and cities. These things communicates wirelessly [1]. Wireless communication as play a very vital role in our daily routine life and it has make our life very easy because it provides communication between different parts of the world with the help of signals that can be radio signals, light signals, Micro signal and infrared without the use of any conductor. Different kind of technologies are used for wireless communication like radio and television broadcasting, Radar communication, satellite communication, cellular communication, GPS system, Wi-Fi, Bluetooth,3G ,4G,5G,HSPA [2].The network type, wireless network is further divided into two parts that is infrastructure Network and infrastructure less network which is also known as wireless ad hoc network. Wireless ad hoc network is then further categorized into two categories there is mobile ad hoc network also known as MANET and the other one is wireless sensor network. The difference between these two is that one is mobile and the other is not. Infrastructure network follow a predefined rules it has for routing that are used to share information between different devices or nodes but in infrastructure less network there is no any predefined rules and structure to differentiate between the nodes and to make communication possible.

- *IqraabidDepartment of computer scienceInstitute of Southern PunjabMultan, Pakistaniabid982@gmail.com:*
- *RanaMudassarrasoolDepartment of computer scienceInstitute of Southern PunjabMultan, Pakistanrazald4m@gmail.com:*
- *Muhammad SaleemDepartment of computer science National College of Business Administration & Economicsidmsaleem@gmail.com*
- *Muhammad Aleem Department of computer scienceInstitute of Southern PunjabMultan, PakistanChishti_aleem@yahoo.com*
- *RiffatHanifDepartment of DPT shahidaislam medical collegelodhranriffathanif1122@gmail.com*

Difference between infrastructure wireless network's types is on the basis of position that some occupy fixed position and some not. Mobile ad hoc network or MANET used dynamic topology while wireless sensor network does not use dynamic rather it use a static topology. The other difference between mobile ad hoc Network and wireless network is that it use heterogeneous network to communicate with each other while in wireless sensor system the network that is used is homogenous means the kind of network can be used must have to be same. In mobile adhoc network The Final Destination is unknown while in wireless sensor system the destination is known and it is that assured that the routing in mobile ad hoc network is based on address which means at it only depends upon the address to share information between nodes while in wireless sensor system it is all dependent upon data.

Infrastructure Wireless networking has many so many benefits. Specifically talk about mobile ad hoc network or MANET it has make our life so very much easier [3]. Having said that, numerous problems and challenges that are attached to this new technology. So, to get benefit from this technology we have to overcome these problems and challenges. Because in infrastructure less wireless network there is no proper infrastructure every node has permission to join the network and leave the network whenever they want to leave and this thing make it more prone to vulnerability [4]. The Other main reason is insecure wireless network because there is no proper security due to wireless network so information that is confidential in nature has more chances to get Leak and intruders may get that information. The other reason due to which wireless Ad Hoc Network get prone to vulnerability is Limited physical security because there are so many nodes that are connected to each other to communicate and send message from one node to another. These nodes might be unprotected or less protected. So due to this unproductive architecture, these are an easy target to be intruded [5]. The Other reason of intrusion is there is no Central management system that provide security like come in wired network so it is also one of the reason [6]. Conventional ways of defense are not enough to cope with different kinds of attacks [7].

2. TAXONOMY RELATED TO SECURITY

Security under the term network includes three major import three major points. One important point is the challenges that occur in security system of any network that is needed to be resolved. The other point is the security requirement that are

considered as requirements needed for a better security system. and the type of attack that can be occur on the basis of their status and behavior and that can influence any security system and leads to vulnerability. The very important security challenges that need to be focused in network security ad hoc network security include threat, physical in security and dynamic nature system [8].

Figure 1Security Taxonomy

Challenges

Infrastructure less network has more chances of attack then wired network. So there are more chances of vulnerability. And attacker might attack more frequently than in any other network. The Attack can be passive or active. If attack is passive in nature then it is more dangerous because it just only keep an eye on our work and then they are preparing for a bigger attack that can damage more than any other. While in active attack, they not only keep an eye on our work but also modify data, delete the data of packets and can consume resources. The other point is a physical in security in mobile ad hoc network physical security is very less or unprotected so that is why they are more prone to be attacked. Physical insecurity is very less and there are two type of attacks that can be committed whether it is internal or external .internal means with in that Network and external means out of that network domain.so ,if attack is within that network domain and then it is more prone to vulnerability rather than external network domain. The other point is dynamic nature of this protocols or network. Due to the dynamic in nature, it has a dynamic topology so static protocols or requirements are not sufficient to fulfill this [9].

Needs

Under the heading of Ad-Hoc networks, network security needs or requirements, the points that need to be focused on availability, authentication, integrity, confidentiality,authorization, and privacy [9]. The very important point is network availability system must granted availability of the data and must have to control the Denial of service attack and make sure that the data is available to the person who demanded that. As shown in Figure, The Other very important point is authentication is means that if two parties want to communicate with each other than the network security must have to check whether they are the same parties who want to communicate and share the confidential data with each other or not. Network security needs is the integrity which means that the data that is shared between the nodes to communicate to the nodes or information that is shared by sender is not malicious .node who is sending information to create a communication is not malicious or intrusion free data. Confidentiality is very important point security. If two parties are communicating with each other they don't want a third party to hear the information or to make it used against them. It is very important need of any security system. Privacy is also very important factor in any communication system to keep confidentiality of parties and their data. The needs in any security system include authorization which is last but not the least .authorization means to provide resources and facilities only to those who authorized actually not those who are unauthorized [10].

Attack Types

The type of attacks that can be performed in network security based on status and behavior .on status basis, The Attack [10] can be internal and external which means that attack has been occurred within that network expressing that malicious node lay within that network domain. External means that that malicious node doesn't lie in a networked domain. Internal attack are more dangerous than external one. On the basis of behavior, attack can be active or passive. Active means that the attacker my change your data, may delete it might modify it. But in passive attack it only keep an eye on our behavior, actions or task [7].

3. IDS Taxonomy

Intrusion detection taxonomy includes the detection process on the basis of different ways and perspectives which includes detection mechanism, response, sources, mode, and detection architecture, frequency of their usage, data types and methods. Intrusion on the basis of response can be active or passive means it can directly affect our work or just spying to get information. Intrusion on the basis of sources means, it can be host base, it happens on host, or network-based, it happens during transmission, or hybrid, both on host and network. Intrusion onthe basis of mode can be online or offline. Online means when a system is connected to internet and offline means when it is not connected to internet. On basis of Collection of data, it can be centralized or distributed. Centralize mean all the data is on a one system or a central system that is accessed by all other nodes. On the other hand, distributed means it is Store on different system or nodes. Intrusion detection system on the basis of frequency means it can be continuous intrusion detection system or periodic. Continuous means it continuously keep an eye on network to detect any kind of intrusion or anomalous behavior. Word periodic means it periodically checks the intrusion while other time it waits [11]. Intrusion detection system based on architecture, include standalone, distributed and cooperative, hierarchical and mobile agent. In standalone detection system, the detection system is installed on a particular node used to detect the intrusion of that system. Distributed and cooperative includes

detection system installed on each and every node but they also share their detection information with their neighboring nodes. In hierarchical detection system, the network layers are divided into different layers containing clusters. Each cluster has a cluster head. Detection systems are install on each and every node but a better detection system is installed on a cluster head. They are collectively used to detect intrusion. While mobile agents are intrusion detection system that are free and can be installed on any system. Mobile agents are used to correlate different activities to detect intrusion [12].

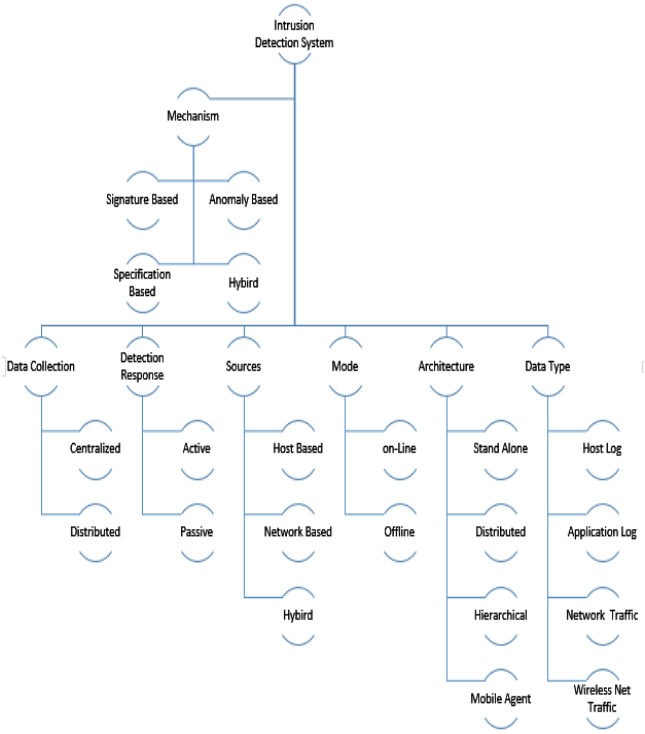

Figure 2Intrusion Detection System Taxonomy [13]

4. IDS Mechanism

On the basis of intrusion detection taxonomy there are so many ways to detect intrusion that include detection mechanism [13], response, mode, architecture, datatype and collection. But detection mechanism will be focused in this survey paper. Detection mechanism includes four type of detection mechanism that includes signature bass or knowledge base, anomaly base, specification base and hybrid that combines these detection mechanism.

Signature Based

In detection mechanism, signature base which is also known as knowledge base is one of the basic type of intrusion detection. It find out patterns that already been found out in the process of intrusion detection. Try to make the use of this pattern to find out or to stop the intrusion that happens particularly of that type. All the intrusion that already been detected are store in a particular database .whenever any other threat or intrusion happens, compare it with the already been detected threats that are store in database. If any threat matches then it reports about that intrusion. As shown in the figure, there is a traffic collector from different sources of processes that could be log file or any other kind of file. Traffic collector collects data and the data that traffic collector found as suspicious will be sent to intrusion detection mechanism based on signature or knowledge. This mechanism matches it with the database that contains already been detected threats. If it is matched then an alarm generates the alert message and report the administrator. If it does not match with the database record, then a mismatch message is generated and will help continue the normal flow.

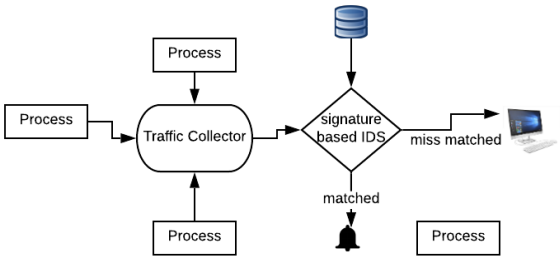

Figure 3 Signature Based IDS

Anomaly Based:

Anomaly based detection mechanism, also known for detecting behavior is used to detect intrusion in MANET. The phenomenon of this detection system is that it keep an eye on normal working or behavior and it learns from the normal behavior and then the system trained from this normal behavior is used to further detect any anomaly by observing the abnormal activity or behavior. Data collected by traffic collector through different processes is used by anomaly based intrusion detection system that has already learned from normal behavior of working flow by observing hosts, data flow and their profiles that are stored in data base. If everything is working fine and there is no any intrusion then it put the false Alarm on and continue the normal working flow. If anything suspicious or abnormal happens, it is sent to threat analyzer. The threat analyzer analyzes whether the threat is known or unknown.in both the cases, it put alarm on and report the threat but in case of unknown threat, it is sent to Learner and there Learner learns from this unknown threat [14].

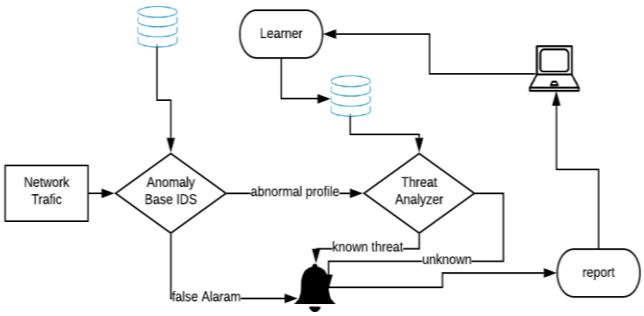

Figure 4 Anomaly Based IDS

Specification Based:

Specific specification based intrusion detection system is same like the anomaly-based system. It is also known as state full intrusion detection system. Difference between state full intrusion detection system and anomaly base system is that in state full intrusion detection system, rules are defined to detect the behavior human. In specification based system behavior is specified by human in the form of rules and that behavior is predefined. If anything happens other than the behavior defined for that, then it percepts that intrusion has been occurred. Its approaches same like anomaly-based

system but only difference is that it includes a manual work by the experts to define rules. Due to the manual work the results of falsepositive rates are lower but it includes an extra overhead and delay [15].

Hybrid:
The last intrusion detection system is hybrid intrusion detection system. This system includes the combination of two other detection mechanism to detect intrusion to get better results and include the advantages of two different mechanism to get better results. It must use two, at least two, detection mechanism that can be specification, anomaly or signature. It has increase the number to detect the intrusion. It has many positive effects on our system. But overhead and overall costs also increases due to the use of different mechanisms.

5. Comparison

Ref	Paper	Architecture	Mechanism	Intrusion Detected	Strength	Weakness
[16]	Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms	Distributive & cooperative	Anomaly	➢ Packet Dropping ➢ Serial Number Modification	➢ Fault Tolerant ➢ Scalable	➢ Complex ➢ Require regular training ➢ More Samples Require
[17]	A survey on intrusion detection and prevention in wireless ad-hoc networks	Distributive & cooperative	Anomaly	➢ Worm Hole	➢ Correctly identify attacker and anomaly	➢ Static environment ➢ Require Long time for training
[18]	BeeAdHoc: An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks Inspired by Bee Behavior	Distributive & cooperative	Hybrid	➢ Malicious and intruder node detection	➢ High Accuracy	Overhead of Communication
[19]	A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols	Distributive based on agent	Anomaly	➢ DoS Attack	➢ High Accuracy ➢ Auto Learn	➢ Large Overhead ➢ No Statistical Analysis ➢
[20]	Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges	Standalone	Anomaly	➢ Flooding ➢ Routing	➢ Optimal Consumption of power	➢ Specificity
[21]	A context adaptive intrusion detection system for MANET	Distributive & cooperative	Specification	➢ DoS Attack ➢ Human Interference	➢ Less False Positive Rate	➢ Un-popular Non Forgery of Mac Address
[22]	A Security Mechanism for Cluster-Based WSN against Selective Forwarding	Distributive & cooperative	Specification	➢ Packet Dropping ➢ Modification ➢ Impersonation	➢ Less overhead ➢ High Accuracy	➢ Performance in unknown ➢ Pre-requisition for analysis of routing protocol
[23]	An Intrusion Detection Tool for AODV-based Ad hoc Wireless Network	Distributive & cooperative	Hybrid	➢ Packet Dropping ➢ Serial Number Modification ➢ More resources usage	➢ No Prior Modification Require For AODV	➢ Impersonation can't be detected
[24]	State Transition Analysis: A Rule-Based Intrusion Detection Approach	Standalone	Specification	➢ Modification ➢ Routing Table Overflow	➢ Less False Positive Rate ➢ Cryptography provides more Security	➢ More resources usage
[20]	Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges	Distributive & cooperative	Anomaly	➢ Packet Dropping ➢ Black hole	➢ More Accuracy ➢ Detect Attacks of different kind	➢ Source of attack can't be detected ➢
[14]	A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud	Distributive & cooperative	Anomaly	➢ Packet Dropping	➢ Initiator of intrusion being tracked	➢ Time and energy consume more ➢ Require proper training and regular training

[25]	GPS-free Positioning in Mobile Ad Hoc Networks	Hierarchical Distributed Architecture	Hybrid	➢ Malicious Node	➢ High Accuracy due to dual detection	➢ More resources usage Overhead increase
[26]	A Reputation-Based Collaborative Intrusion Detection Network to Lessen the Impact of Malicious Alarms	Distributive & cooperative	Anomaly	➢ Compromised and Attacker Node	➢ Remove attacker node	➢ More Alarm overhead of false Positive
[27]	Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks	Distributive & cooperative	hybrid	➢ Black hole ➢ Packet Dropping ➢ Resource Consumption	➢ High Accuracy due to dual detection	➢ More Network Traffic
[28]	Outlier detection methods for identifying network intrusions – A survey	Standalone	Anomaly	➢ DoS Attack	➢ High Accuracy	➢ Consume More Resources
[15]	An Efficient Multi Level Intrusion Detection System for Mobile Ad-Hoc Network Using Clustering Technique	Standalone	Anomaly	➢ Selfish Node	➢ Attractive strategy	➢ In-efficient
[29]	Using Bayesian Game Model for Intrusion Detection in Wireless Ad Hoc Networks	Distributive & cooperative	Anomaly	➢ Jamming	➢ Attacks are Blocked more accurately and correctly	➢ Consume More Resources ➢ Not suitable for Larger Networks

6. Discussion

Comparison has been made between different mechanisms that is used by ad hoc network intrusion detection system. The comparison shows that Different techniques has been used that shows it has resolved different kind of attacks. On the basis of comparison that has been made so far in these papers. The mechanism that has been used the most is anomaly based mechanism that has helped to detect most of the attacks and it has some strong points and weak points. attack that has resolved it shows that it has resolved so many attacks like black hole , selective packet drop, flooding, denial-of-service ,routing modification, grey hole and many other this attacks have been resolved the outcome shows that it has low overhead and it provides more accuracy in results anomaly based system provides Cryptography so it has more computational overhead. Some of the system, detection is complex and it need regular training. on the other hand, specification mechanism The Attacks that are resolved include packet dropping ,impersonation, resource consumption, table overflow etc. it includes the benefits of low false positive rate , secure due to cryptographic techniques. Its weaknesses prerequisite of routing protocol it is very unpopular and due to Cryptography demand larger computational power. The hybrid is used by combining other mechanism to achieve better result but it increases the overhead double the time. But it has more advantages than any other.

7. Conclusion

In this paper, we have describe different security issues or Threats that need to be resolved, requirements related to security. In Survey paper we have focused on the mechanism aspect of intrusion detection system that how many mechanism are being used, what purpose it has been used, and what are the goals that have been achieved with that mechanism. Comparison is also given in this paper that shows different strong points, weak points and the attack that have been resolved. Based on this comparison, we have concluded some Intrusion detection mechanism that are more better than other in some of the cases and the type of attacks a security threat that has been resolved. Basis on the survey we have find out some of the areas that need to be focused that includes the privacy of parties communicating with each other. Because it is the security need that must have to be kept on top priority.

REFRENCES

[1] Z. A. Almusaylim, A. Alhumam and N. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review," Ad Hoc Networks, p. 102096, 2 2020.

[2] "TypesnUses.com," 9 december 2019. [Online]. Available: https://www.typesnuses.com/different-types-wireless-communication-technologies/. [Accessed 6 3 2020].

[3] Y. Singh and S. Kumar Jena, "CCIS 203 - Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad Hoc Networks".

[4] C. Pu, S. Lim, J. Chae and B. Jung, "Active detection in mitigating routing misbehavior for MANETs," Wireless Networks, vol. 25, no. 4, pp. 1669-1683, 1 5 2019.

[5] M. T. Scholar, A. Gupta and N. Ranjan, "A Survey of Attacker Identification and Security Schemes in MANET".

[6] G. Singh, T. Narendra, S. Chaudhari, J. Luis, V. Barbosa, M. Kumar and A. Editors, "International Conference on Intelligent Computing and Smart Communication 2019 Algorithms for Intelligent Systems".

[7] M. N. Lima, A. Luiz, D. Santos and G. Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks".

[8] V. Goyal and G. Arora, "Review paper on security issues in mobile Adhoc networks," International Research Journal of Advanced Engineering and Science, vol. 2, no. 1, pp. 203-207, 2017.

[9] U. Amin and A. Shah, "A Novel Authentication and Security Protocol for Wireless Adhoc Networks".

[10] M. A. Ferrag, L. Maglaras and A. Ahmim, Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey, vol. 19, Institute of Electrical and Electronics Engineers Inc., 2017, pp. 3015-3045.

[11] H. Debar, M. Dacier and A. Wespi, "Towards a taxonomy of intrusion-detection systems," 1999.
[12] C. Xenakis, C. Panos and I. Stavrakakis, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks," Computers and Security, vol. 30, no. 1, pp. 63-80, 1 2011.
[13] S. X. W. a. W. Banzhaf, ""The use of computational intelligence in intrusion detection systems: a review," Applied Soft Computing, vol. 1, pp. 1-35, 2010.
[14] O. Singh, J. Singh and R. Singh, "An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes," Indian Journal of Science and Technology, vol. 10, no. 14, pp. 1-12, 1 4 2017.
[15] A. A. Korba, M. Nafaa and S. Ghanemi, "An efficient intrusion detection and prevention framework for ad hoc networks," Information and Computer Security, vol. 24, no. 4, pp. 298-325, 2016.
[16] A. Mitrokotsa, M. Tsagkaris and C. Douligeris, "Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms".
[17] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," Journal of Systems Architecture, vol. 105, 1 5 2020.
[18] H. F. Wedde, M. Farooq, T. Pannenbaecker, B. Vogel, C. Mueller, J. Meth and R. Jeruschkat, "BeeAdHoc: An Energy Efficient Routing Algorithm for Mobile Ad Hoc Networks Inspired by Bee Behavior," 2005.
[19] N. Mazhar and M. Farooq, "A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols," Applied Soft Computing Journal, vol. 11, no. 8, pp. 5695-5714, 12 2011.
[20] S. Kumar and K. Dutta, Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges, vol. 9, John Wiley and Sons Inc., 2016, pp. 2484-2556.
[21] "S1383762118306246".
[22] H. Zhou, Y. M. Wu, L. Feng and D. Liu, "A security mechanism for cluster-based WSN against selective forwarding," Sensors (Switzerland), vol. 16, no. 9, 20 9 2016.
[23] G. Vigna, S. Gwalani, K. Srinivasan, E. M. Belding-Royer and R. A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks".
[24] K. Ilgun, R. A. Kemmerer and P. A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection Approach," 1995.
[25] S. Capkun, M. Hamdi and J.-P. Hubaux, "GPS-free Positioning in Mobile Ad Hoc Networks," 2002.
[26] M. Gil Pérez, F. Gómez Mármol, G. Martínez Pérez and A. F. Skarmeta Gómez, "RepCIDN: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms," Journal of Network and Systems Management, vol. 21, no. 1, pp. 128-167, 3 2013.
[27] P. Kabiri and M. Aghaei, "Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks," 2011.
[28] J. R. Beulah and D. Shalinipunithavathani, "Outlier detection methods for identifying network intrusions-A survey," 2015.
[29] H. Wei and H. Sun, "Using Bayesian Game Model for Intrusion Detection in Wireless Ad Hoc Networks," International Journal of Communications, Network and System Sciences, vol. 03, no. 07, pp. 602-607, 2010.
[30] ICET 2012 : 2012 International Conference on Emerging Technologies, 8-9 October, 2012, Islamabad, Pakistan., IEEE, 2012.
[31] W. J. Chung and T. H. Cho, "A Multi-Path Routing Determination Method for Improving the Energy Efficiency in Selective Forwarding Attack Detection Based MWSNs," International Journal of Wireless & Mobile Networks, vol. 10, no. 4, pp. 09-19, 30 8 2018.
[32] H. Cheng and J. Cao, "I E E E C O M M U N I C AT I O N S A DESIGN FRAMEWORK AND TAXONOMY FOR HYBRID ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS," 2008.
[33] Y.-A. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," 2003.
[34] R. Gupta, S. Tanwar, S. Tyagi and N. Kumar, Machine Learning Models for Secure Data Analytics: A taxonomy and threat model, vol. 153, Elsevier B.V., 2020, pp. 406-440.
[35] I. PES Institute of Technology (Bangalore, IEEE Communications Society, IEEE Photonics Society. Bangalore Chapter, IEEE Robotics and Automation Society. Bangalore Chapter and Institute of Electrical and Electronics Engineers, 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) : 19-22 Sept. 2018..
[36] M. Safaei, S. Asadi, M. Driss, W. Boulila, A. Alsaeedi, H. Chizari, R. Abdullah and M. Safaei, "A Systematic Literature Review on Outlier Detection in Wireless Sensor Networks," Symmetry, vol. 12, no. 3, p. 328, 25 2 2020.
[37] W. :. Www, D. G. Kariya, A. B. Kathole and S. R. Heda, "International Journal of Emerging Technology and Advanced Engineering Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method," 2012.
[38] S. X. Wu and W. Banzhaf, The use of computational intelligence in intrusion detection systems: A review, vol. 10, 2010, pp. 1-35.
[39] F. H. Tseng, H. P. Chiang and H. C. Chao, "Black hole along with other attacks in MANETs: A survey," Journal of Information Processing Systems, vol. 14, no. 1, pp. 56-78, 2018.
[40] B. Subba, S. Biswas and S. Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," Engineering Science and Technology, an International Journal, vol. 19, no. 2, pp. 782-799, 1 6 2016.
[41] D. g. Zhang, J. x. Gao, X. h. Liu, T. Zhang and D. x. Zhao, "Novel approach of distributed & adaptive trust metrics for MANET," Wireless Networks, 2019.
[42] K. Bala, A. Chandra Sekar, M. Baskar and J. Paramesh, "An efficient multi level intrusion detection system for mobile ad-hoc network using clustering technique," International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 1977-1985, 1 8 2019.