Research Article

A Review of the cluster based Mobile Adhoc Network Intrusion Detection System

T. Sushma[1], G. Chenchamma[2], B V Subbayamma[3], Nagendra Babu Rajaboina[4]

[1]Assistant Professor, Prasad V Potluri Siddhartha Institute of Technology
[2]Principal, Vijaya institute of Technology for women
[3]Assistant Professor, Prasad V Potluri Siddhartha Institute of Technology
[4]Assistant Professor, Vijaya institute of Technology for women
[1]tsushmaece@gmail.com, [2]vijayatechfw@gmail.com, [3]kolla.samyuktha@gmail.com,
[4]nagendrarajaboina@gmail.com

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: The Mobile Ad-hoc Network is decentralized and consisting of numerous different communication devices. Its distributed design and lack of infrastructure are the means of numerous network assaults. For personal computer users, companies, and the military, network security has become more important. Safety becomes a significant issue with the rise of the internet, and the past of security enables a better understanding of the evolution of security technology. Via the audit and monitoring phase, the implementation of Intrusion Detection Systems (IDS) in ad-hoc node securities was improved. This framework is made up of clustering protocols that are extremely efficient in finding intrusions with low resource and overhead computing costs. Current protocols have been related to routes that are not popular in intrusion detection. The cluster is barely impacted by the weak road layout and route renewal. The cluster is unpredictable and results in processing maximization together with network traffic. In general, battery-based ad hoc networks are organized and dependent on power constraints. To detect and react rapidly against intrusions, an active monitoring node is required. Only if the clusters are strong and extensive maintaining capabilities can it be accomplished. The routes also shift as the cluster shifts and it would not be feasible to prominently process the achievement of intrusion detection. This raises the need for a better clustering algorithm that addresses these disadvantages and guarantees the protection of the network in any way. A powerful clustering algorithm that is ahead of the current routing protocol is the cluster-based Intrusion Detection Method. Regardless of routes that perfectly track the intrusion, it is permanent. This streamlined technique of clustering achieves strong intrusion detection speeds with low processing as well as memory overhead. It also overcomes the other limitations of traffic, connections, and node mobility on the network, regardless of the routes. In detecting the attack or malicious node, the individual nodes in the network are not active.

Keywords: Network Security, MANET, CBIDP, DRINA Intrusion, Cluster, Malicious Node, Ad Hoc Networks.

1. Introduction

With the introduction of the Internet and modern networking technologies, the planet is getting increasingly inter-connected. Networking infrastructures worldwide provide a vast volume of personal, commercial, military, and government knowledge. Due to intellectual property that can be quickly accessed via the internet, network protection is being of considerable significance. Network protection, typically with a username and a password, begins with authorization. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Network protection essentially means allowing access to data on a network that is managed by the network administrator. For personal computer users and organizations, it has become more important. If allowed a firewall forces network user to access protocols, such as what networks should be reached. This part can fail to review potentially dangerous material, such as computer worms or trojans transmitted over the network, to prevent unauthorized access to the device. The malware is detected using anti-virus tools or an intrusion detection device (IDS). Today, a phenomenon such as wire shark traffic will still track the network and can be logged for audit purposes and subsequent high-level device review. To preserve privacy policies, cryptography can be used to interact between two hosts utilizing a network.

It is distributed architecture which requires on a broad spectrum of MANET (Mobile Ad-Hoc Networks) that have a significant influence among the many analysis realms. It has accomplished a steady growth in the market in recent years, the explanation behind this is its different application fields such as mobile conferencing, battlefield, and disaster relief operations, etc. The competitive design allows the week of the scheme and proposes several attacks as a potential route. No set topology is followed for the Ad-hoc network, since it is dispersed in nature. In the network, in the processing of packet forwarding individuals, a particular node is both the host and the router. Unlike infrastructure-based wireless networks, there is no ad-hoc base station, and the network node nodes will travel freely in any direction. At any moment, these nodes in the network will join or exit. While it has some benefits, there are still several serious problems such as protection and power limitation. This is because the battery and strength of these networks are constrained. The main limitations of the long-standing process are the manufacturing capabilities and reduced power. For this cause, by contributing a large

amount of power, more networks with nodes are needed for the forwarding of packets throughout the network. The shortage of unified monitoring points, the absence of complex topology and restricted bandwidth are significant problems that make the network susceptible to multiple attacks. Because of these protection violations, they often suffer from authentication, spoofing, eavesdropping, access protection, denial of service, etc., as well as wired communications [21]. Moreover, it also has selfishness, dark hole, sinkhole, sleep loss, wormhole, etc. owing to the wireless existence, there is a severe shortage of current ad hoc protocols and they suffer from scrambling, manufacturing, etc. Equally trusting all nodes, including the intermediate node, is the essential problem in the ad-hoc, from which it may easily produce or monitor the data packets and make detecting MANET interference a task.

2. Types of Attacks

The basic class of attacks that can cause slow network efficiency, unregulated traffic, viruses, etc. is defined in this section. Network Threats by Malicious Nodes. Attacks may be divided into two categories: "Passive" where a network attacker intercepts data passing across the network, and "Active" when an intruder initiates orders to impede the regular activity of the network.

2.1. Active Attacks

Spoofing intrusion, Wormhole attack, Alteration, Denial of Services, Sinkhole, and Sybil attack are several successful threats.

1. Spoofing: Forgetting the name of a hostile node, such that the sender switches the Topology.

2. Modification: When a malicious node modifies the routing route, such that the sender sends the message down the long path. This assault creates contact delays between the sender and the recipient.

3. Wormhole: The tunneling attack is often referred to as this attack. An intruder obtains a packet at one stage in this assault and tunnels it to another malicious node in the network. So, a novice believes that he has discovered the shortest route on the network.

4. Fabrication: The fake routing message is generated by a malicious node. This implies that incorrect route information is produced between devices.

5. Connection denial: In a service denial attempt, the malicious node sends a request to the node and uses the network bandwidth. The primary target of the malicious node is for the network node to be busy. If a message arrives from an unauthenticated node, the message would not be answered by the recipient because he is occupied, and the novice must wait for the recipient's answer.

6. Sinkhole: Sinkhole is a service attack which prevents full and correct data from being obtained by the base station. A node attempts to draw the data from his all-neighboring node to it in this assault. Through using this attack, selective alteration, forwarding or lowering of data can be achieved.

7. Sybil: Several copies of malicious nodes related to this attack. Since the malicious node shares its secret key with other malicious nodes, the Sybil attack may take place. In this way, the number of malicious nodes in the network is increased and the risk of attack is therefore increased. If multipath routing is used, so the capacity to pick a malicious node route would be improved throughout the network.

2.2. Passive Attacks

Traffic tracking, Eavesdropping, and Surveillance are the titles of certain passive assaults.

1. Traffic analysis: An intruder attempts to sense the contact route between the sender and the recipient during the traffic analysis attack. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

2. Eavesdropping: This is a proactive threat, which happened in the handheld ad-hoc network. The key purpose of this assault is to uncover any knowledge through contact that is classified or confidential. The confidential information could be the sender or receiver's private or public key, or other secret details.

3. Monitoring: In this attack, the intruder can read sensitive data, but is unable to modify the data or change the data.

3. Literature Survey on Cluster Based Ids

In recent years, Mobile Ad-hoc Network security has become a highlighted issue among the research community via massive growth. Different analysis scholars have dedicated their work to improving MANET protection from earlier until today.

M. Elbasiony [1] proposed hybrid structure, the anomaly part is improved by replacing the k-means algorithm with another algorithm named the weighted k-means algorithm, additionally, it uses a suggested approach to pick the anomalous clusters by introducing proven attacks into unknown data links. S.A. Joshi [2] implemented to resolve these current network issues, data mining-based IDS is opening new res res. Data mining is used to find new trends which were not identified previously from wide amount of network dataset. Sannasi Ganapathy[3] a survey on intelligent strategies for feature discovery and classification for intrusion detection in networks focused on intelligent software agents, neural networks, genetic algorithms, neuro-genetic algorithms, fuzzy techniques, rough collections, and particle swarm intelligence has been proposed. Panos Louvieris [4] introduced a novel anomaly detection method that can be used to detect previously unknown attacks on a network by defining threat attributes. In order to improve the situational knowledge of cyber network operators, this effect-based feature recognition approach uniquely incorporates k-means clustering, Naive Bayes feature option and C4.5 decision tree classification for pinpointing cyber-attacks with a high degree of precision. A traffic flood assault detection and an in-depth research method that uses data mining techniques were suggested by Jaehak Yu [5]. A detailed study of DDoS threats, detection methods and instruments used in wired networks was provided by Monowar H. Bhuyan [6]. The paper also outlines open questions, study issues and potential solutions in this field. Iftikhar Ahmad [7] shows that many methods to intrusion detection are usable, but their efficiency is the key issue, which can be strengthened by growing detection rates and decreasing false positives. The emphasis of study in this paper is this question of the current techniques.

Wenying Feng [8] implemented a new data classification algorithm focused on machine learning that is applied to the identification of network interference. A new method blends SVM with Self-Organized Ant Colony Network (CSOACN)-based clustering to take advantage of each thus preventing their vulnerabilities. A new intrusion detection method focused on the KK-nearest neighbor (KK-nearest neighbor, referred to as KNN) wireless sensor network classification algorithm was proposed by Wenchao Li [9]. By analyzing their irregular activities, this system may distinguish abnormal nodes from regular nodes. A new support vector machine (SVM) model combining kernel principal component analysis (KPCA) with genetic algorithm (GA) was suggested by Fangjun Kuang [10] for intrusion detection. Roshan Chitrakar [11] suggested a half-partition method for the collection and preservation of non-support vectors in the current classification increase, called Nominee Support Vectors (CSV), which are likely to become support vectors in the next classification increase. In order to classify the appropriate, secret data of interest to the consumer easily and with less execution time, Nadiammai [12] implemented a data mining concept that is combined with an IDS. Algorithms such as the Powerful Data Adapted Decision Tree (EDADT) algorithm, Hybrid IDS model, Semi-Supervised Solution and Variant Hopping Time Alignment and Modification (HOPERAA) have been proposed. A modern hybrid intrusion detection system has been implemented by Gisung Kim [13] that hierarchically combines a model of misuse detection and an anomaly detection model is proposed in a decomposition framework. A game theoretical tool, namely cooperative game-based Fuzzy Q-learning, was provided by Shahaboddin Shamshirband [14] (G-FQL). In WSNs, G-FQL adopts a mix of both the game theoretical method and the fuzzy Q-learning algorithm. Eun Hee Jeong [15] suggested an IP

Trace back Protocol (ITP) focused on network forensics against network attacks that uses a Compressed Hash Table, a Sinkhole Router and Data Mining.

A systemic and automatic approach to developing a hybrid IDS was proposed by Shengyi Pan [16], which learns temporal state-based requirements for power system scenarios, including delays, regular control activities, and cyber-attacks. For the whole Advanced Metering Infrastructure (AMI) device consisting of individual IDSs for three separate tiers of AMI elements, Mustafa Amir Faisal [17] suggested a practical and efficient IDS architecture: smart meter, data concentrator, and AMI head end. Salma Elhag [18] considered the usage of Genetic Fuzzy Structures inside an IDS pair-wise learning context. He benefits of utilizing this method are twofold: first, the use of fuzzy sets, and specifically linguistic marks, makes for a clearer borderline between the

definitions and allows the rule set to be more interpretable. Second, the divide-and-conquer learning method, in which we contrast all potential pairs of groups with targets, increases the precision of unusual attack cases, since it achieves a greater separability between a "normal activity" and the different forms of attack. Adel Sabry Eesa [19] proposed a new approach to function selection focused on the algorithm of cuttlefish optimization used for intrusion detection (IDSs). The proposed model uses the cuttlefish algorithm (CFA) as a search technique to decide the best subset of features and the classifier of the decision tree (DT) as a judgement on the chosen features generated by the CFA. Khattab M. Ali Alheeti [20] has developed an intrusion detection mechanism to detect Denial of Service (DoS) attacks for VANETs utilizing Artificial Neural Networks (ANNs).

Zhang et al. [22] applied a standardized solution to intrusion prevention in Ad-hoc networks. He notes that in defining the intrusions, nodes are autonomous and cooperate in situations, as necessary. But the downside is that the invasive activities cannot be inferred precisely from a single node. The local, global detection engine and answer modules are run by individual nodes in this method, which renders the process more complicated. Around the same time, the knowledge to be processed is enormous by implementing dynamic multilayer integration, thereby optimizing computing capacity and intense computation. Li et al. [23] have suggested a new approach for mobile agents (MA) in the intrusion detection scheme in protection science. In his work, the approach to intrusion detection effectively in a network was orchestrated via MA technology. The boss, assistant and answer mobile agents were processed in the network monitoring and intrusion warning. It allows the design overhead for a single node with immense intrusion data and makes the operation repetitive with a vast amount of storage space.

Yi-an et al. [24] have established a cooperative intrusion mitigation technique for MANETS. For the run-time resource restriction problem, the author discussed cluster-based intrusion detection technique in this work. Cluster head collection and creation was controlled by the cluster head and clique computing protocol for cooperative intrusion detection. It needs bi-directional connections in the clique computing protocol, which results in a maximum number of elections and HELLO messages by connectivity exchanges. Different clustering algorithms were suggested to provide effective routing while contemplating enhancing safety standards in the MANET. However, some of these algorithms were addressed in [26, 27, and 28] and the distributed existence of rendering routing complex. The Watchdog method is known in the scientific community as the foundation for several intrusion prevention strategies coined by Sergio Marti et al [30]. Utilizing the Watchdog system, the MANET misbehavior node is effectively identified but the forward packets are approved. Various problems such as receiver collision, restricted control of transmitting, inaccurate reporting of wrongdoing, unclear collision, and partial fall render it impossible for Watch Dog to locate the presence of the hostile node in the network. Parker et al built Route rater and Improved Watchdog on the study journey after Watchdog [33] (ExWatchdog). In this work, he concentrated on the vulnerability of the Watchdog system by means of the routing protocol [31]. For each node, Ex-Watchdog is structured with tables to manage the number of packets sent and retrieved over the network. The Path rater is a hybrid approach with Watchdog that proposed a modern intrusion detection and response scheme [32] for route guard. Two response modes were built in this system, known as passive response mode and active response mode. CONFIDENT, another process developed by Sonja Buchegger et al, is regarded as Cooperation of Nodes Justice in Complex Ad-hoc Networks [34]. Any single node in the network handles four significant components, namely a reputation scheme, confidence manager, control, and route manager, by applying Sure. A method abbreviated as 'CineMA' that processes Cooperation Enhancement in MANET, handles and regulates misbehaving nodes with few packets forwarded as defined in [35].S. A novel cluster-based malicious node identification method using the combination of cluster key and cluster head was suggested by Gopalakrishnan et al.[36]. During the exchange, the cluster head tests whether the cluster key is true, which allows for safe transmission. Moreover, the author fixes the link loss triggered by the inclusion of the malicious node.

4. Cluster Based Intrusion Detection

4.1. Cluster Formation and Cluster Agent Election

The creation of a cluster separates the network into many manageable units, each of which is responsible for the observation and weak processing of the network. A particular type of node is labelled as a 'Head Node' (HD) in the clustering technique and is responsible for tracking traffic within its cluster. For network-wide communication, it manages and interacts with other clusters and handles all node and neighbor cluster information. The management of the cluster revolves around competent participants who are responsible for preserving the equilibrium of load, fault tolerance [26] and must be equal and safe [24]. By holding daily elections between the cluster member nodes, a proper accomplishment is accomplished. The election method is

clear and does not include any details on the computation of the clique or neighboring information [25, 24 and 27]. At regular intervals, the cluster-head holds every referendum, in which all nodes will engage in voting and demonstrate their interest in being the cluster-head. The high-voted and eager node will be the cluster-head before the next timeout cycle (or proves the strongest according to any criteria). A quick overview of the clustering algorithm with an examination of node states, data structures, HELLO messages, the method of appointing the cluster head (election) and checking votes and outcomes, as defined in [25]. The findings reveal that the suggested ID clustering scheme [25] is a lesser-than-scheme cluster [24].

4.2. Intrusion Detection System Planning

An attack attempt is made or is not identified by IDS on a network or a device. It conducts audit results, analyses, and takes proactive steps such as blocking and/or notifying the device administrator of the intruder. In clustered audit points, ad hoc networks have big disadvantages, rendering the usage of IDS critical in a dispersed way [29, 30]. It minimizes the complexities of the node, such as computing and overhead memory, etc. On the network, IDS may be implemented as host-based or network-based based on the need for monitoring standard. The deviation or misuse/signature in the network is a method that has been applied. Every host traffic is controlled by the host-based IDS (HIDS), while the network-based IDS (NIDS) is located at different points along the network. Centralized audit points are not presented in ad hoc networks, and NIDS is unlikely. Via HIDS, each host continues to track the intrusions separately, including the use of tremendous memory as well as computation. A distributed and combined methodology must be used for a proper management mechanism in the network to resolve this. Both the head and participant nodes gather knowledge. The IDS is a rare and ideal option for the identification of abuse programs. The method of misuse identification is specific to established trends of unlawful behavior. For the identification of intrusions by the 'natural' operation baseline, the anomaly detection method is applicable and processes this with 'self-learning'[31]. Normally, in many instances, if the database is not modified, the misuse identification method struggles to locate the assault signatures. The other concerns with the misuse identification method are that it generates a large archive which creates memory restriction issues by collecting all the identified suspicious signatures. The anomaly detection strategy was fairer since it trained with regular traffic with the passing of time. The knowledge is often used for the identification of irregular activities/behavior throughout the testing phase.

Both logs and traffic during the transition is obtained by the HD node in a network by its radio range. It stored the appropriate fields on the database, such as all collected traffic in the promiscuous mode. Traffic may be data traffic or traffic management, storing all traffic linked to data, such as the number of packets sent, obtained, redirected, or lost. RERR packets are the power traffic of the AODV, RREQ, RREP, ELECTION and HELLO CBID packets. It is easy to identify multiple attacks, such as a black hole, wormhole, packet falling, sleep deprivation and malicious flooding, by holding these records. The route specifics were reported by member nodes (MB) and gateway nodes (GW), respectively, such as the number of routes added, deleted, etc. In addition, these capabilities often render it possible to track other threats, such as denial of service (SYN flooding) and path manufacturing attacks. We use several parameters such as packet transformation, mobility, throughput, and end-to-end pause with many nodes to evaluate the output of the device.

5. Conclusion

We reviewed several researchers' approaches to intrusion detection clustering schemes in WSN and adhoc networks in this article. A study area in the field of security risks for WSN and ad hoc networks is proposed in this report. The Cluster Based Intrusion Detection Framework provides an easy yet highly safe method for intrusion detection and monitoring. This system combines the formation of clusters and the election of cluster agents with a planning map for intrusion detection.

By way of its anonymous actions, the cluster head works effectively to identify malicious nodes in a network. Based on that, the numerous variables such as swift, secure, selection process, management, and prevention can be evaluated. There are still challenges to solve in executing these widespread context-aware applications.

References

1. M. Elbasiony, Reda, *et al*, “A hybrid network intrusion detection framework based on random forests and weighted k-means,” *Ain Shams Engineering Journal*, Vol. 4, No. 4, pp.753-762, 2013.
2. S. A. Joshi and Varsha S. Pimprale, "Network Intrusion Detection System (NIDS) based on data mining," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol.

2, No. 1, pp. 95-98, 2013.

3. Sannasi Ganapathy, *et al., "*Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, Vol.1, pp.271, 2013.
4. Louvieris, Panos, Natalie Clewley and Xiaohui Liu, "Effects-based feature identification for network intrusion detection," *Neurocomputing*, Vol. 121, pp. 265-273, 2013.
5. Jaehak Yu, *et al.*, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques," *Journal of Systems Architecture*, Vol.59, No.10, pp.1005-1012, 2013.
6. Monowar H. Bhuyan, *et al., "*Detecting distributed denial of service attacks: methods, tools and future directions," *The Computer Journal*, Vol.57, No.4, pp.537-556, 2013.
7. Iftikhar Ahmad, *et al., "*Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components," *Neural computing and applications*, Vol.24, No.7-8, pp.1671-1682, 2014.
8. Wenying Feng, *et al., "*Mining network data for intrusion detection through combining SVMs with ant colony networks," *Future Generation Computer Systems*, Vol.37, pp.127-140, 2014.
9. Li, Wenchao, *et al., "*A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, 2014.
10. Kuang, Fangjun, Weihong Xu and Siyang Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," *Applied Soft Computing*, Vol.18, pp.178-184, 2014.
11. Roshan Chitrakar and Chuanhe Huang, "Selection of candidate support vectors in incremental SVM for network intrusion detection," *computers & security*, Vol.45, pp.231-241, 2014.
12. G. V. Nadiammai and M. Hemalatha, "Effective approach toward Intrusion Detection System using data mining techniques," *Egyptian Informatics Journal*, Vol.15, No.1, pp.37-50, 2014.
13. Gisung Kim, Seungmin Lee and Sehun Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, Vol.41, No. 4, pp. 1690-1700, 2014.
14. Shamshirband and Shahaboddin, *et al., "*Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Engineering Applications of Artificial Intelligence*, Vol.32, pp.228-241, 2014.
15. Jeong, Eun Hee and Byung Kwan Lee, "An IP Traceback Protocol using a Compressed Hash Table, a Sinkhole router and data mining based on network forensics against network attacks," *Future Generation Computer Systems*, Vol.33, pp.42-52, 2014.
16. Shengyi Pan, Thomas Morris and Uttam Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, Vol.6, No.6, pp.3104- 3113, 2015.
17. Mustafa Amir Faisal, *et al., "*Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," *IEEE Systems journal*, Vol.9, No.1, pp.31-44, 2015.
18. Elhag, Salma, et al, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," *Expert Systems with Applications*, Vol.42, No.1, pp.193-202, 2015.
19. Eesa, Adel Sabry, Zeynep Orman and Adnan Mohsin Abdulazeez Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, Vol.42, No.5, pp.2670-2679.2015.
20. Alheeti, Khattab M. Ali, Anna Gruebler and Klaus D. McDonald- Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," *Consumer Communications and Networking Conference (CCNC)*, 2015 12th Annual IEEE. IEEE, 2015.
21. P. Albers et al., "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches", in Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002), Apr, 2002.
22. Yongguang "Intrusion Detection in Wireless Ad-Hoc Networks" , Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Mobi-Com 2000, Boston, Massachusetts, Aug 6 11, 2000, pp 275-283.
23. Chunsheng Li et al., "MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents", Proceedings of the 2nd International Conference on Information Technology for Application (ICITA), 2004.
24. Yi-an Huang "A Cooperative Intrusion Detection System for Ad Hoc Networks", in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia, October 31, 2003.

25. Kashan Samad et al., "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks", 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, September 15-17, 2005.
26. S. Banerjee "A Clustering Scheme for Hierarchical Control in Wireless Networks", in Proceedings of IEEE INFOCOM, 2001
27. Mingliang Jiang et al., "Cluster Based Routing Protocol (CBRP)", Internet Draft, Jul, 1999.
28. P. Krishna et al., "A cluster-based approach for routing in dynamic networks", ACM SIGCOMM Computer Communication Review, 27(2):49-64, 1997.
29. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks" proceedings of the 6th Annual International Conference on Mobile Computing and Networking Mobicom '00 , pp.255-265, August 2000
30. N, Chen. Y, "Enhanced Intrusion Detection System for Discovering Malicious Node in Mobile Adhoc Networks" Communications, 2007. ICC'07. IEEE International Conference on, Vol.10, pp.1154-1159, 24-28, June 2007.
31. Hasswa.A et al., "An Intrusion Detection and response system for mobile ad-hoc networks" wireless and mobile computing, networking and communication, IEEE International Conference on, Vol 3,pp. 336- 343, August 2005.
32. Arker.J et al., "On Intrusion Detection and Response for mobile Adhoc Networks", performance, computing and communications,2004 IEEE International Conference, pp.747-752, 2004
33. S. Buchegger "Performance Analysis of the Confident rotocol cooperation of Nodes: Fairness in Dynamic Adhoc Networks", in MOBIHOC '02, 2002 .
34. M. Frank et al., " Cinema: Cooperation enhancement in MANETS", in proceedings of the 29th Annual IEEE International Conference on Local computers Networks LCN'02, 2004
35. Ejaz Ahmed et al., "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks" NUST Institute of Information Technology (NIIT), Rawalpindi, Pakistan.
36. S. Gopalakrishnan, P. Mohan Kumar "Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET", Circuits and Systems, 2016, 7, 748-758.