Performance Evaluation of Intrusion Detection System based on LDK, NCA Algorithms and GBC Method

D. Nethra Pingala Suthishni, Anna Saro Vijendran

Abstract: The growth of wireless technology has concerned the necessity of Intrusion Detection System (IDS). To pact with a several arising security impacts and other problems in the communication atmosphere. Many of the researchers had developed several algorithms to cope with the malicious things in Mobile Ad hoc Networks (MANETs). Supervision of the network behavior IDS have to run all over the network and all the time on every node. This approach is costly overhead for mobile device and computational resources. These devices are powered by batteries in terms of power. Least Degree for K (LDK), Node Categorization Collaboration among the nodes are accomplished by the implementation of algorithm Node Categorization Algorithm (NCA) and Grid Based Clustering (GBC) algorithms that will reduce the time delay and overhead process. Validation approach of improved Intrusion Detection system is compared with the GBC approaches. The Improved IDS model confesses intrusions and malicious nodes in DSR Protocol.

Keywords: Detection Accuracy, Intrusion Detection, Least Degree for K, Node Categorization Algorithm.

I. INTRODUCTION

A huge immense development in communication technologies and models that support the advancement of mobility as well as self-organization is witnessed by the past decade. MANETs is an illustration of self-organized and self-configured networks where there are no concentrator units that are gateways. The MANET environment consists of nodes with highly dynamic as they join and leave the network at any time [4]. However, such network designs are vulnerable to diverse attacks. Several challenges have been raised to preserve the MANET that is free from the action of faulty nodes or malicious nodes. In the face of the difficulty of avoiding the effects of malicious activities in the network system, some of the rectifying mechanisms are necessary. These are essential at least to minimize such effects on the network system. Intrusion detection systems (IDSs) can be used as one of the mechanisms to minimize the effect of malicious attacks [5]. IDS communication system depends on the co-operation of nodes that rely on the network and that do not belong to the system. Many of the network-based research works focus mainly on problems applied to traditional routing protocols in MANETs [1] and some works focus on the issues of malicious behavior [5][7][1-2].

In a network or any network-based system, any type of unapproved or unauthorized activity is called intrusion. An IDS is a compilation of methods, resources, and tools. It is used to identify, assess, and report intrusions in the network system. Normally in any Intrusion Detection System, one part of a protection system is installed around a system or device to protect the device from the intrusion and intruders. It is not a stand-alone protection measure [8] for securing the device. Intrusion prevention methods such as secure routing, encryption, access control, authentication, etc. are presented as the first line of protection against intrusions [12]. In any category of security schemes in the transmission over the network, interference cannot be completely rectified. The interference in the network leads to loss of confidential or any secret information such as protection keys being exposed to the illegitimate user. Intrusion effects in the malfunction of the defensive security mechanism of the system. Therefore, IDSs are intended to expose intrusions, before the intruder disclose the secured system of resource that is confidential information. One of the most considered walls of protection from the point of security in IDS. Cyberspace and IDSs are comparable to the burglar alarms which are implemented in to the physical security systems today [9].

In the network, security level is monitored and optimized with the incorporation of LDK's minimum degree of neighbor nodes. Every node in the network has to monitor the value of security with its LDK probability. In this approach only limited neighbor involves in the instant monitoring. Security and tradeoff are the prominent features of LDK. Monitoring nodes increases in respect to the security level. By inheriting the challenges distributed IDS is developed.

Consider that random number of L-data packets is transmitted among control packets and at the same time attacker will consistently drop the packets. Grid Based Clustering Algorithm partitions the network area in to equivalent size of grid cells and constrained of the square region. Cluster head is elected from the one of the nodes in the grid cell which is nearest to the grid cell's center. Among all other nodes in the grid cell, the node which has a minimum distance to the midpoint of the grid cell is chosen to be CH. GBC is used to reduce the energy hole problem and heavy traffic.

Revised Manuscript Received on December 16, 2019.

***** Correspondence Author

D. Nethra Pingala Suthishni*, Department of Computer ScienceSri Ramakrishna College of Arts and Science, Coimbatore, India. nethra.phd.snr@gmail.com

Anna Saro Vijendran, Department of Computer Science Sri Ramakrishna College of Arts and Science, Coimbatore, India.

II. INTRUSION DETECTION SYSTEM

An IDS is a software application or device that monitors the network or a system for any malicious activity or legal policy violations. Any legal policy violation or malicious activity is usually either collected centrally or reported to an administrator. This process is done by the security information and event management (SIEM) system and merges the results from various sources that utilizes the alarm filtering technique to differentiate malicious activity from false alarms in the network. Representation as well as the classification of IDS is network-based or host-based scheme. Depending on the type of mechanism employed on data collection, IDS is identified. Host-based IDS runs on the operating system's audit trails, application logs where audit data are created by loadable-kernel modules that interrupt system calls in this system. The network-based IDS system operates on packets captured from network traffic. . IDS is based on the detection technique as classified in the below diagram.

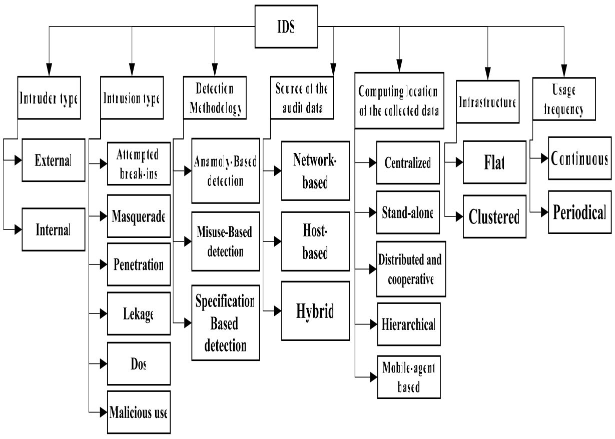

Figure 1. Classification of IDS [3]

- **Signature-based Method:** signature based ids finds the attacks based on specific patterns such as number of 1 s 0 s and number of bytes in the network traffic. this method also works on the basis of the already known malicious instruction sequence that is used by the malware or other kinds of intrusions. The detected patterns are known as signatures. Signature-based IDS are capable of detecting the attacks. The system is difficult to detect new malware attacks.
- **Anomaly-based Method:** Anomaly-based IDS is initiated for identifying unaware malware or other types of attacks towards the network. Prominent activity model is modelled by the machine learning technology.

It is stated as suspicious if it is not found in the model. The machine learning-based method has an efficient generalized property in comparison to signature-based IDS. It is according to the applications and hardware configurations.

- **Specification-based:** It explains a set of designs that explains the exact operation of a network scheme or protocol and monitors the execution of the program with reverence to the definite constraints. Specification Based method may give the ability to identify formerly unknown attacks while they try to attempt a low false positive rate.

Abbreviations and Acronyms

- **Pfa** - Probability of false alarm
- **Pmd** - Probability of miss-detection
- **Perror** - Overall detection-error probability
- **PGB** - Link error rate
- **PBG** - Packet loss rate
- **Ldata** - Random number of Ldata data packets are sent between two consecutive control packets.

Units

- Unit of the energy is (Joule/S)
- Unit of the packet dropping is (drop/S)\
- Unit of Overall detection error probability (Random packet/S)
- Unit of Miss Detection Probability (Random Packets/s)
- Unit of False Alarm Probability (Random Packets/s)
- Unit of Impact of Control Packet Dropping Rate (Control Packets/s)
- Unit of Impact of L-data (Control Packets/s)
- Unit of Impact of PGB (Control Packets/s)
- Unit of Random Packet Drops (Drop/s)
- Unit of Impact of Sample Packets (Drop/s)
- Unit of Selective Packet Drops (Drop/s)

Equations

- Overall detection = Pgb / Pgb + Pbg
- Miss-Detection probability (Pmd) = Imd / 1000
- False-Alarm probability (Pfa) = Ifa / 1000
- Control Packet Dropping rate = CDL - Mdp
- L-data = 1 / (1 - PBG)
- PGB = Tpkt – Spkt
- Random Packet Drops = Mpkt * Gpkt
- Sample Packet = Bs * Ra
- Selective Packet Drops = Hdp + Ldp

III. COMPARATIVE STUDY OF IDS

Active time of IDS in every individual node of the network is diminished by the LDK algorithm. In order to attain the energy utilization effectively LDK is incorporated in the mobile network. Higher level of security features are achieved by integration of IDK in to IDS. More amount of energy necessity to establish without the involvement of any prominent structure [9].

Node Categorization Algorithm (NCA) came in to the category of a supervised learning method. Multivariate data is segregated in to distinct classes with the help of NCA. Distance metric over the data flow in the network enables the categorization of NCA and it aims at "learning" a distance metric. Identification of a linear transformation of input data helps to study the values. NCA is used for finding the optimal solution and best path in the WSN[13].

GBC Algorithm partitions the network area in to equal size of grid cells and it is constrained of the square region. Cluster head (CH) is selected from the one of the nodes in the grid cell which is nearest to the grid cell's center. Grid cell is composed of several nodes that have only smallest distance from the midpoint of the grid cell which is chosen by the CH. The broadcast of data are initiated by the primary CH. The location and the energy represent the presence of the nodes. Further transmitting nodes are identified by the primary CH. Transmission scheduling and reception is done by CH [9].

Related Works

Ahmed.E, Samad.K, &Mahmood.W [1], illustrated the IDS that provides the ability to watch over the transmission medium and audit the security nodes in the local area. Renovation and establishment of route may consequences the cluster as well as influences. Non stable cluster may raise traffic and processing overhead. MANETS are subjected to several constraints likely power and security. Designed clustering scheme is used for the detection of intrusion, low processing, memory overhead and high detect rates. The IDS is irrespective of routes, connections, traffic types, and mobility of nodes in the network.

Bononi.L, and Tacconi.C [2] explained wireless scenarios IDS and secure routing methods that is initiated for ever-increasing security and reliability. The authors have depicted an integrated routing scheme based on IDSs as well as Statistically Unique and Cryptographically Verifiable (SUCV) identifiers. The developed IDS is used for the maintenance of secure Ad Hoc On-Demand Distance Vector (AODV) routing which is named as IDS-based Secure AODV (IS-AODV), in wireless ad hoc and other application oriented vehicular network developments. Recognition of anomalies behavior on behalf of neighbor hosts is based on IDS, with passive reactions. Author aiming to build a cluster whose route paths will comprise only protected nodes.

Huang, Y. A., & Lee, W. [3] explained the progress in developing intrusion detection (ID). Anomaly detection approach is improved to give more details on the source and attack types. Simple rules can be applied to finding numerous well-known attacks and attackers. A cluster-based recognition scheme with a run-time resource-limited problem in that cluster head is chosen based on the periodical value. Each node in the network has a unique agent ID. Maintaining the level of effectiveness is enriched with the help of the agent ID generation method. Experiments were conducted extensively using the ns-2 and MobiEmu environments to evaluate the efficiency of the research.

Kachirski, O., &Guha, R [4] analyzed malfunction for the entire WSN and tried to inhibit the attempts of intrusion. Generally, IDS are developed for wired networks. The authors have applied an proficient and bandwidth-conscious framework that targets intrusion at several levels. Here, the network takes account of the distributed nature of ad hoc WSN management and decision policies.

Ping, Y., Xinghao, J., Yue, W., &Ning, L. [5] designed a timed automaton for MANET's DSR protocol that incorporates distributed intrusion detection methods. Nodes within the cluster were chosen based on the periodical values and the chosen nodes monitor the transmission. Selected nodes supervise the global as well as local intrusion detection systems. Timed automata are generated manually for abstracting the exact activities of the node in relevance to the dynamic source routing (DSR). The supervising nodes can confirm the behavior of every node by timed automata, and without signatures of intrusion real-time attacks were validly noticed. Each node in the architecture owns a unique IDS agent. Finally, the intrusion detection technique is assessed through simulation experiments. The agent-based method shows efficiency and effectiveness.

Nadeem.A,&Howarth.M [6] explained a combination of anomaly-based and knowledge-based IDS to protect the MANETs variety of attacks. It can detect new unforeseen attacks. The authors also investigated the algorithm's impact on the MANET to check the performance of the various attacks and the type of intrusion response and established the necessity for an adaptive intrusion response.

Ngadi .M,Abdullah .A.H, and Mandala .S [7] elucidated the security problems on MANET that has become one of the most prominent concerns. The MANET is more susceptible to be attacked than wired networks. The authors aim to investigate and to categorize present methods of the IDS among MANET environments. To maintain these ideas, a discussion concerning attacks, IDS architectures, and research has been made and also some enhancements are achieved on MANET and are presented inclusively. The authors also insist that comparison can be made among several types of research in the future and that will be evaluated based on these parameters.

Kotiswaran Thanigaivelu and Krishnan Murugan [8] stated WSN data's are fixed state sink routing. Fixed sinks in the sensor nodes transmit all the available data from the sensor nodes. Energy hole issue and network's life span are reduced due to the heavier traffic as well as data load. Cluster configuration is established by a novel approach Grid-based clustering (GBC). GBC uses dual CH namely primary and secondary to improve the efficiency of the network. GBC can be applied to anytype pf network.

A. Performance Metrics

Overall Detection - Error Probability

In the context of decision making and transmission, the probability of error may be measured as being the probability of making improper transmission or a wrong decision and that would have a different value for every type of error probability. [13]

Formula for Error Probability

Intruder in the network hides the packet in the background that is drops through the link errors by evading the transmission channel is called as overall detection error probability.

Overall detection = Pgb / Pgb + Pbg

Pgb - Link error rate,

Pbg - Packet loss rate

Miss Detection Probability

The probability that secondary transmission in the network may misses at the time of any primary transmission due to the noise and channel fading. Any malicious activity may also arouse these types of errors [14].

Formula for Miss Detection Probability

One of the enviable network transmission contexts is miss detection probability. In the transmission area malicious nodes are identified in a higher probability.

Miss-Detection probability (Pmd) = Imd / 1000

Imd - Attacker is not present time calculate drop

False - alarm Probability

It is the probability of false detection of the data transmission when the source node is silent in the current transmission medium [10].

Formula for False - alarm Probability

The faintly higher false-alarm rate should not be a problem, because in the post-detection investigation phase a false alarm can be easily recognized and fixed.

False-Alarm probability (Pfa) = Ifa / 1000

Ifa - packet-loss bitmaps and collect the number of cases

Impact of Control Packet Dropping Rate

Dropping packets is undesirable and either lost during the transmission or must be retransmitted to the wrong route and impact throughput; however, increasing the buffer size can lead to buffer bloat which has its collision on latency and jitter during congestion [11].

Formula for Impact of Control Packet Dropping Rate

Packet dropping that is the loss of packet during data transmission is managed by detection accuracy. Packet drop is identified at the data packet losses and the correlated control. This context plays vital role in the uplift of detection accuracy.

Control Packet Dropping rate = CDL - Mdp

CDL - Control and data packet drop

Mdp - Malicious packet Drops

Impact of L-data

Transmission of data packets among any two successive nodes (L-data) is called as L-data.

Formula for Impact of L-data

Consider that random number of L-data packets is transmitted among control packets and at the same time attacker will consistently drop the packets.

L-data = 1 / (1 - PBG)

PBG - Packet loss rate

Impact of PGB

During the transmission of any packets from source to destination are the transition probabilities from good to bad and from bad to well given by PGB.

Formula for Impact of PGB

Deterioration in detection accuracy can increase the PGB value.

PGB = Tpkt – Spkt

Tpkt - Total no of Packet loss

Spkt - Source of Packet loss

Random Packet Drops

Random packet drop is losing occurs when one or more packets. The data is transmitting the network fail to reach their destination.

Formula for Random Packet Drops

Detection error rises with the block size in many cases. As a larger block size hides more details of packet losses, and therefore makes the definite correlation of lost packets more complicated to compute.

Random Packet Drops = Mpkt * Gpkt

Mpkt - Most recent packet sent,

Gpkt - Generates a packet-reception

Impact of Sample Packets

In order to attain consistency in detection accuracy two methods are carried namely sample packets are fixed to formulate the sample blocks. The sample blocks are fixed in respect to the block size.

Formula for Impact of Sample Packets

Sample Packet = Bs * Ra

Bs - Decreases with the block size, Ra - Does not reduce the amount of computation

Selective packet Drops

Selective packet drop attack is associated with DoS attacks. Malicious nodes in the network trigger the DoS attack. Many techniques have been developed to segregate selective attacks from the network. It sends 10packets [9].

Formula for Selective packet Drops

Loss of packets between the range of high and low packets is selective packet drop.

Selective Packet Drops = Hdp + Ldp

Hdp - High packet dropping rate

Ldp - Low packet dropping rate

B. Result and Discussion

When comparing the detection accuracy attained by the newly designed algorithm using DSR protocol with IDS algorithm, only shares the number of lost packets is utilized. Assume that the packets are spread constantly over this hop [11]. Finally, the performance metrics for without IDS and With IDS schemes are compared with various node densities.

Table I. Simulation Parameters

S.NO	Metrics	IDS
1	No of nodes	100
2	Routing Protocol	DSR
3	Routing Protocol Queue Type	CMUPriQueue
4	Initial Energy	100(J)
5	Data Packet Size	300 bytes
6	MAC Type	Mac/802_11
7	IDS Propagation	1.58%
8	Traffic Type	Constant bit rate
9	Mobility	Low
10	Range of X axis	1000
11	Range of Y axis	1000
12	Simulation Ending Time	65ms

Table II. Simulation Result for Detection Accuracy

Metrics	Overall Detection Error Probability (Random Packets/s)		Miss Detection Probability (Random Packets/s)		False Alarm Probability (Random Packets/s)	
Time	**Exist**	**Propose**	**Exist**	**Propose**	**Exist**	**Propose**
5	1.6	1.6	1.6	1.6	1.02	1.02
10	1.25026	1.23049	1.35026	1.33049	1.50974	1.5395
20	1.25024	1.23027	1.35024	1.33027	1.50976	1.53991
30	1.25023	1.22824	1.35023	1.32824	1.50977	1.54209
40	1.18286	1.1612	1.28286	1.2612	1.58197	1.60902
50	1.01681	1.00518	1.01681	1.00518	1.48681	1.53981

Table III. Simulation Result for Detection Accuracy for control packet drops

Metrics	Impact of Control Packet Dropping Rate (Control Packets/s)		Impact of L-data (Control Packets/s)		Impact of PGB (Control Packets/s)	
Time	**Exist**	**Propose**	**Exist**	**Propose**	**Exist**	**Propose**
5	1.6	1.6	1.6	1.6	1.02	1.02
10	1.30058	1.28099	1.40026	1.38049	1.48942	1.50901
20	1.30053	1.28055	1.40024	1.38027	1.48946	1.50946
30	1.30051	1.27832	1.40023	1.37824	1.48949	1.51281
40	1.23303	1.20117	1.33286	1.3212	1.56178	1.57105
50	1.02696	1.00516	1.02681	1.00518	1.57696	1.61489

Table IV. Simulation Result for Detection Accuracy for block-based algorithms

Metrics	Random Packet Drops (Drop/s)		Impact of Sample Packets (Drop/s)		Selective Packet Drops (Drop/s)	
Time	**Exist**	**Propose**	**Exist**	**Propose**	**Exist**	**Propose**
5	1.02	1.02	1.02	1.02	1.02	1.02
10	1.47943	1.49902	1.46943	1.48902	1.45943	1.47902
20	1.47947	1.49946	1.46947	1.48946	1.45947	1.47946
30	1.47949	1.50281	1.46949	1.49281	1.45949	1.48281
40	1.55178	1.58105	1.54178	1.56105	1.53178	1.54105
50	1.57696	1.61489	1.58196	1.61489	1.57696	1.61489

Above Table II shows the Comparison of Detection Accuracy in Random Packet Drop, Table III shows the Comparison of Detection accuracy for control packet drops and Table IV shows the Comparison of Detection accuracy of block-based algorithms

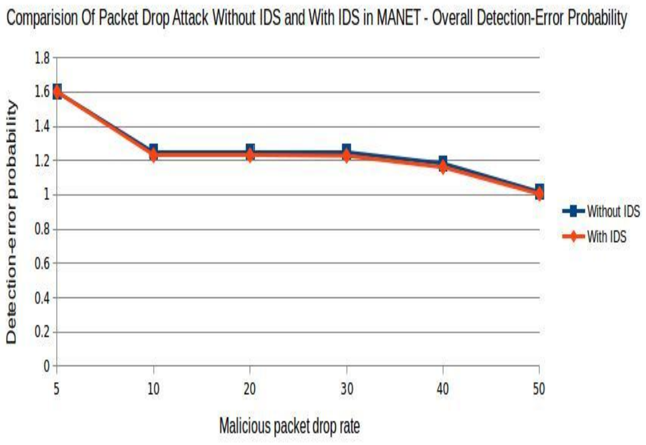

Figure 5: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Overall Detection-Error Probability

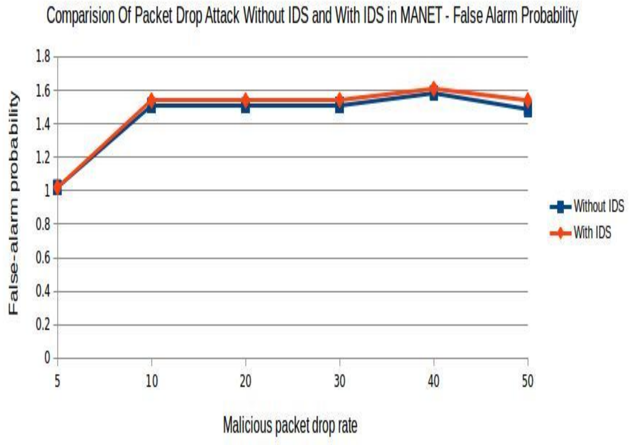

Figure 6: Comparison of Packet Drop Attack without IDS and with IDS in MANET - False - alarm Probability

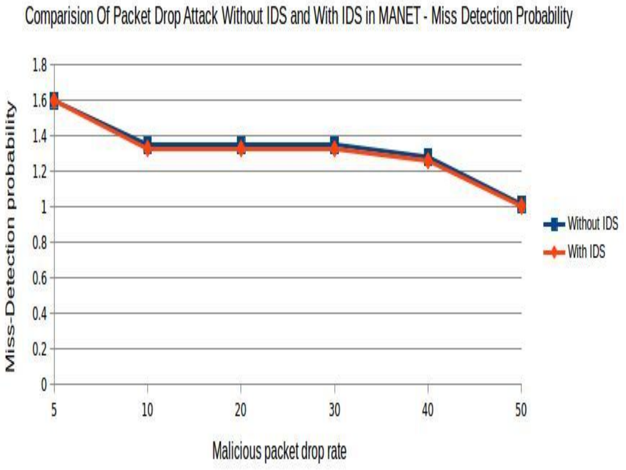

Figure 4: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Miss Detection Probability

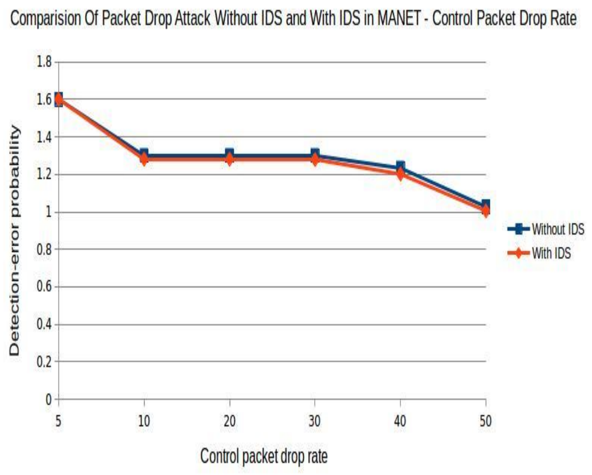

Figure 7: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Impact of Control Packet Dropping Rate

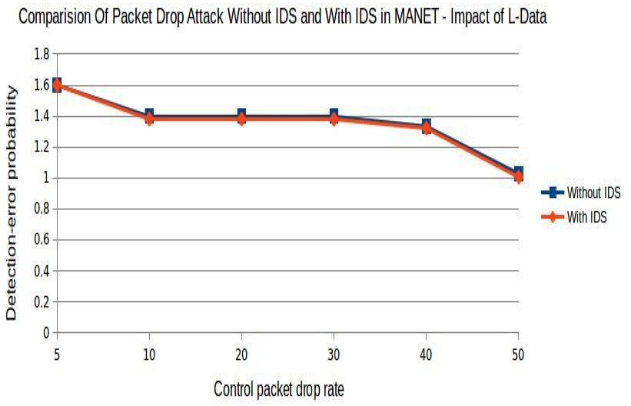

Figure 8: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Impact of L-Data

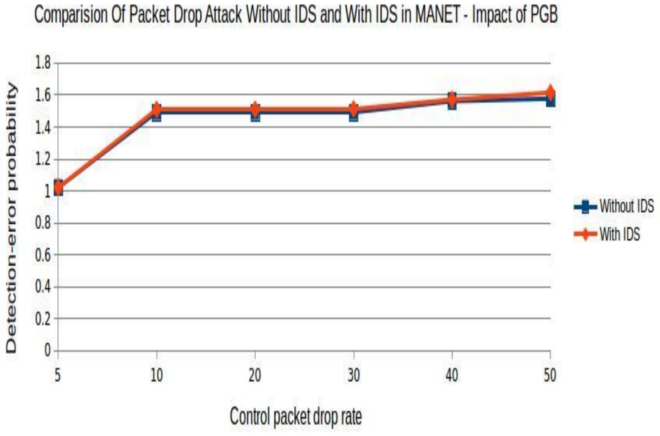

Figure 9: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Impact of PGB

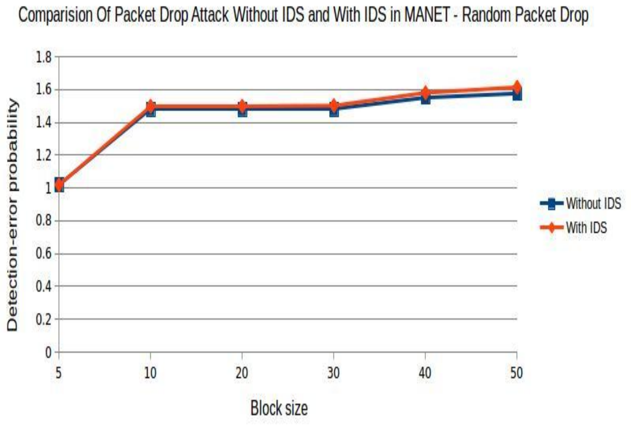

Figure 10: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Random Packet Drop

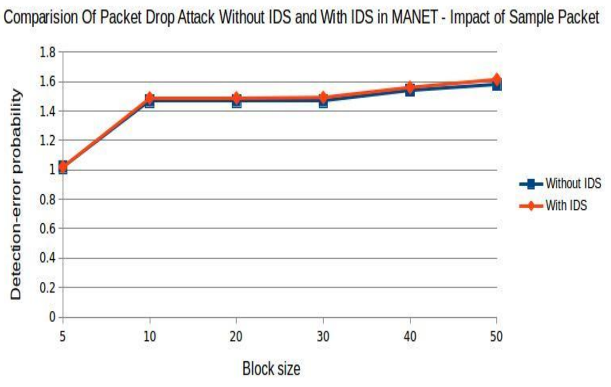

Figure 11: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Sample Packets

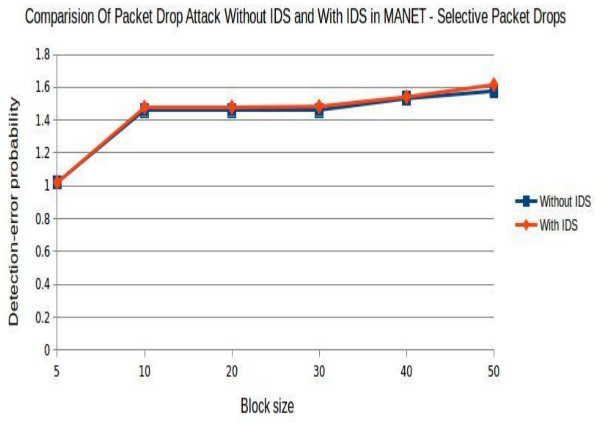

Figure 12: Comparison of Packet Drop Attack without IDS and with IDS in MANET - Selective packet Drops

IV. CONCLUSION

An effective intrusion detection technique is LDK with NCA and GBC algorithms are compared in this paper. The IDS approach uses the Least degree for-K (LDK) algorithm to minimize the individual active time and Node categorization algorithm to find the optimal path. IDS aims at finding the occurrences against networks and computer systems. In general, against information systems are prevented by IDS. IDS can be viewed as a protector of the network system that automatically detects malicious activities within a host or network. In this paper, IDS that exploits only the dispersal of the count of lost packets. It utilizes the association among lost packets considerably that enhances the correctness in discovering malicious packet drops is compared with existing algorithms.

REFERENCES

1. Ahmed.E, Samad.K, &Mahmood.W, “Cluster-based intrusion detection (CBID) architecture for mobile ad hoc networks”, In 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006.
2. Bononi.L, &Tacconi.C, “Intrusion detection for secure clustering and routing in mobile multi-hop wireless networks”, International journal of information security, Vol. 6(6), pp. 379-392, October 2007.

3. Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (pp. 135-147). ACM.
4. Kachirski.O, &Guha.R,"Effective intrusion detection using multiple sensors in wireless ad hoc networks",In 36th Annual Hawaii In ternational Conference on System Sciences, January 2003.
5. Ping, Y., Xinghao, J., Yue, W., &Ning, L. (2008). Distributed intrusion detection for mobile ad hoc networks. *Journal of systems engineering and electronics*, *19*(4), 851-859.
6. Nadeem.A, &Howarth.M, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", Telecommunication Systems, Vol. 52(4), pp. 2047-2058, April 2013.
7. Ngadi .M, Abdullah .A.H, and Mandala .S, "A survey on MANET intrusion detection", International J.Computer Science and Security, Vol. 2(1), pp. 1-11, February 2008.
8. Kotishwaran Thanigaivelu and Krishnan Murugan,"Grid-based Clustering with Predefined Path Mobility for Mobile Sink Data Collection in WSN", IETE TECHNICAL REVIEW, Vol.29 (2), pp. 133-147,MAR-APR 2012.
9. Sherin Joy C." Grid Based Energy Efficient Multipath Routing Protocol In Wireless Sensor Network Using Fuzzy Approach". International Journal of Engineering Research & Technology (IJERT), Vol.3(4), pp.1122-1126,April 2014.
10. https://www.igi-global.com/dictionary/miss-detection-probability/46227
11. https://en.wikipedia.org/wiki/Packet_loss
12. Receivedfromhttps://en.wikipedia.org/wiki/Neighbourhood_components_analysis
13. https://www.igi-global.com/dictionary/probability-of-false-alarm-/46090
14. https://en.wikipedia.org/wiki/Probability_of_error

AUTHORS PROFILE

D.NethraPingalaSuthishni received her MCA Degree from SNS College of Technology(Anna University),Coimbatore in 2009, Master of Philosophy in Computer Science from Hindusthan College of Arts and Science (Bharathiar University) in 2013, Coimbatore.She is a research scholar in Sri Ramakrishna College of Arts and Science (Formerly SNR Sons College), Coimbatore and currently working as Temporary Teaching Assistant in the Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women. Her research areas are Networking and Soft Computing.

Dr. Anna SaroVijendran received her MCA Degree from University of Hyderabad in 1988, Master of Philosophy in Computer Science from ManonmaniamSundaranar University in 2003, Tirunelveli and Doctor of Philosophy in Computer Science in the area of Digital Image Processing and Neural Networks from Mother Teresa Womens University, Kodaikanal in 2009. At present, she is the Dean in School of Computing, Sri Ramakrishna College of Arts and Science (formerly SNR Sons College), Coimbatore. Her research interests are in the fields of Image Processing, Artificial Neural Networks, Computer Networks, Data and Image Mining. As on date, 77 number of her research papers have been published in various Journals (UGC Approved, Scopus, SCI). In addition, she has presented 52 research articles in National and International Conferences. Further, two books namely "Design and Development of Efficient Multipath Routing Protocol in Mobile Ad-hoc and Sensor Networks" and "An Ontology Based Image and web page Retrieval for knowledge Extraction using SABC-SEB Clustering" have been published. She has also been the author for two chapters in books published by leading publishers. She is a Member of the Computer Society of India. She has been the Reviewer and Programme Committee member in International conferences conducted in various countries. She has acted as Chair Person in National and International levels. Apart from that she has visited Cairo, Malaysia and Singapore for presenting her Research Articles. For her credit, she received the "IARDO Award for Excellence 2018" from International Association of Research and Developed Organization, "Instrumental Role for SPOC Award" from NPTEL, IIT, Madras, "Best Faculty Senior Award" from Sri Ramakrishna College of Arts and Science and "Best Paper Award" in various conferences. She is recognized as Research Supervisor in various Universities and acted as Convener & Member of the Inspection committee of Bharthiar University. As on date, she has produced 11 Ph.D. Scholars and 11 M.Phil. Scholars.