ISSN:0975-9646

Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network

Husain. Shahnawaz[1], Gupta S.C.[2],

[1]*Graphic Era University, Dehradun(U.K) India*
[2]*Prof. Emeritus IIT Roorkee (U.K.) India.*

***Abstract*-- Ad-hoc network is a collection of mobile nodes that are capable of dynamically form a temporary network without the support of any centralized fixed infrastructure. Since there is no central controller to determine the reliable & Secure communication paths in Adhoc Network, each node in the ad hoc network has to rely on each other in order to forward packets, thus highly cooperative nodes are required to ensure that the initiated data transmission process does not fail. In a mobile ad hoc network where security is a crucial issue and they are forced to rely on the neighbor nodes, trust plays an important role that could improve the performance of the network. Larger the number of trusted nodes, higher successful data communication process rates could be expected. In this paper, a friendship model is used & evidence through experiments on how a friendship concept could be used to minimize the number of false alarms raised in MANET Intrusion Detection System (IDS). Feature extraction and rule induction to find out the accuracy of detection engine by deploying support vector machine.**

Keywords—Intrusion Detection System, Adhoc Network, Trust level, Gids, Lids, UTC, APF.

I. INTRODUCTION

Intrusion detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges [18]. Experience teaches us never to rely on a single defensive line or technique. IDSs, by analyzing the system and user operations in search of activity undesirable and suspicious, can effectively monitor and protect against threats Numerous detection techniques and architecture for host machines and wired networks have been proposed. A good taxonomy of wired IDSs is presented in [19]. With the rapid proliferation of wireless networks and mobile computing applications, new vulnerabilities that do not exist in wired networks have appeared. However, the vast difference between wired and wireless networks make traditional intrusion detection techniques inapplicable. Wireless IDSs, emerging as a new research topic, aim at developing new architecture and mechanisms to protect the wireless networks. Attacks in Mobile Adhoc networks can be categorized as provided in Table I.

TABLE I
LIST OF UTC & APF

1. Unfair use of the transmission channel (UTC)	2. Anomalies in Packet Forwarding (APF)
• Ignoring the MAC protocol • Jamming the transmission channel with garbage • Ignoring the bandwidth reservation scheme • Malicious flooding • Network Partition • Sleep Derivation	• Drop packets • Blackhole Attack • Gray hole Attack • Delay packet transmissions • Wormhole Attack • Packet dropping • Routing Loop • Denial of Service (DoS) • Fabricated route messages • False Source Route • Cache Poisonings • Selfishness • Spoofing

In MANETs, intrusion prevention and intrusion detection techniques need to complement each other to guarantee a highly secure environment. They play different roles in different status of the network. Intrusion prevention measures, such as encryption and authentication, are more useful in preventing outside attacks. When a node is compromised, the attacker owns all its cryptographic key information, therefore, encryption and authentication cannot defend against a trusted but malicious user at this time the role of intrusion detection is more important.

II.RELATED WORK

Reputation based schemes detect misbehaving nodes and notify other nodes of the misbehaving nodes. Incentive based approaches aims to promote positive behavior to foster cooperation instead of relying on participants to report and punish misbehaving nodes. Zhang et al. [14] has developed a distributed and cooperative intrusion detection system (IDS) where individual IDS agents are placed on each and every node. Each IDS agent runs independently, detects intrusion from local traces and initiates response.

Bhargava and Agrawal [16] have extended the IDS model described in [2] to enhance the security in AODV (Ad-hoc on demand Distance Vector) routing protocol. Watchdog [3] proposes to monitor packet forwarding on top of source routing protocols like DSR. Watchdog has the limitations of relying on overhearing packet transmissions of neighboring nodes for detecting anomalies in packet forwarding. [17] follows the concept of [3] but works with ADOV. It adds a next hop field in AODV packets so that a node can be aware of the correct next hop of its neighbors. It also considers more types of attacks, such as packet modification, packet duplication, and packet-jamming DoS attacks. Each independent detection result is signed and flooded; multiple such results from different nodes can collectively revoke a malicious node of its certificate, thus excluding it from the network. Bal Krishnan [8] has proposed a way to detect packet dropping in ad-hoc networks that addresses the problems of receiver collisions, limited transmission power.

Model given in [1] is derived from previous research provide evidence on how a friendship mechanism could be used to improve the accuracy of IDS in MANET [6]. One of the main issues in MANET IDS is on the number of false alarms raised in the network as a result of false claims/reports made by individual nodes. This anonymity problem is a big challenge in MANET because it is difficult for nodes to distinguish between trusted and un-trusted nodes in such autonomous networks.

III. PROPOSED FRAME WORK

In [1] some assumptions that each node has a list of initial trust and that will be shared with the other nodes present in the network these initial trust list can be generated on behalf of profile database shown on figure-1. These initial lists are known as Direct Friend Mechanism (DFM).

TABLE III
NODE'S INITIAL TRUST

Node ID	Initial Trust
A	B & C
B	C,D,E
C	A,D,B
D	C,B
E	A,C

A. *IDS Alarm Analysis*

This provides four possible results for each traffic trace analyzed by the IDS

True Positive (TP) when the attack succeeded and the IDS was able to detect it

(Success ^Detection)

True Negative (TN) when the attack failed and the IDS did not report it

(¬Success ^ ¬ Detection)

False Positive (FP) when the attack failed and the IDS reported on it

(¬ Success ^ Detection)

False Negative (FN) when the attack succeeded and the IDS was not able to detect it **(Success ^ ¬ Detection)**

B. In [1], IDS model is divided into two sub-model one is Local IDS and another is Global IDS and they follow the 20:80 Rule to speed up their detection rate in the Lids the thresh hold value is set very high in the detection engine to detect the highly malicious node. Lids uses Feed Back Table (FBT) to provide the collective result from Unfair use of Transmission channel based detection engine (UDE) and Anomaly Based Detection Engine (ADE) Table 3. Profile data base will maintain the trusted neighbor list generated by Lids and this list is again used in Gids for rigorous checking for rest of the rules in which Threshold value of detection engine is set to detect normal intruder behavior.

TABLE III
FBT

UDE	ADE	Value
0	0	0
0	1	1
1	0	1
1	1	1

After completing the detection engine process data collected from Gids and indirect profile will collectively decide the trust level on behalf of voting scheme given in Table IV.

TABLE IV
TRUST LEVEL GENERATED BY GLOBAL DETECTION ENGINE

Node Id	Trust Level
A	2/5
B	3/5
C	4/5
D	2/5
E	1/5

In this research, Trust Level is generated, and on behalf of this Trust level individual nodes can decide to include the participation of node which has lowest trust level in different processes like routing, and deciding the cluster head for scalable adhoc networks.

C. *Feature Selection*

Feature Selection in the area of intrusion detection can be found in [20], [22], where standard feature selection techniques (forward / backword

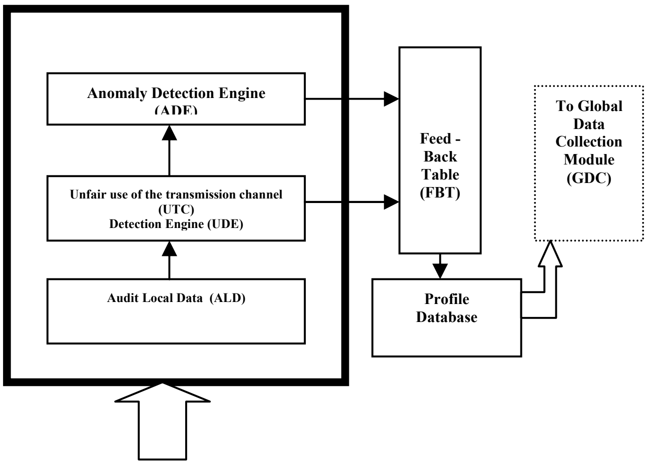
Anomaly Detection Engine (ADE)
Unfair use of the transmission channel (UTC) Detection Engine (UDE)
Audit Local Data (ALD)
Feed - Back Table (FBT)
Profile Database
To Global Data Collection Module (GDC)

Fig. I. Lids[1]

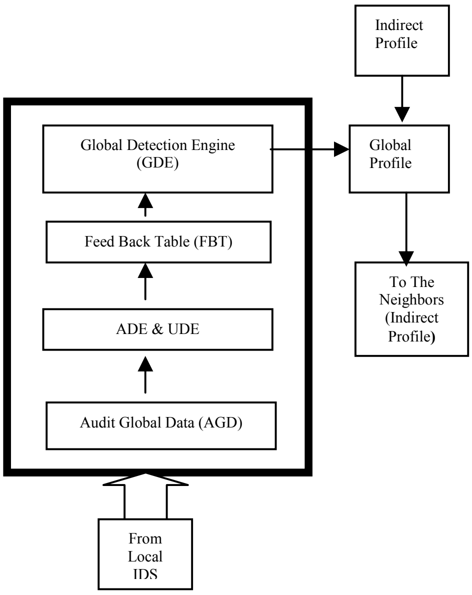

Fig. II Gids[1]

search, beam search or sequential search) are applied in combination with decision trees and keyword based IDS, In order to recognize attacks and to distinguish between normal and intrusive behavior, 137 different features can be extracted from TCP/IP header & can be grouped into 19 different categories [9] and given in the table-VI, on behalf of Table VI different category of attacks can be classified according to these features in Table-V

TABLE-V
ATTACKS ON BEHALF OF TCP/IP HEADER FEATURES

Guest / R2L	F-5,F-12,F-14
DoS	F-7,F-12,F-19
Port Sweep	F-7,F-12,F-13,F-14
N-Map	F-5,F-13,F-12,F-14
IP-Sweep	F-5,F-7,F-19

Guest / Remote to Local (R2L) Login: an attacker, who does not have an account on a victim machine, gains local access to the machine, exfiltrates files from the machine, or modifies data in transit to the machine.

If TTL is same from the different packets with FIN bit is ON and RST bit is also on.

DoS: DoS attack may be possible with different variety but in current situation we consider the case of TCP/IP header.

If Segment Header with full capacity and start hour is busy hour and RST bit is ON.

Port Sweep: is the method to probe a server or host for open ports and the not working ports to launch the zombie.

If TCP/IP header with default or minimum value and SYN/FIN bit is ON.

Ping sweep/ IP Sweep: is a technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP ECHO requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. A ping is often used to check that a network device is functioning.

SYN scan is another form of TCP scanning, the port scanner generates raw IP packets itself, and monitors for responses. This scan type is also known as "half-open scanning", because it never actually opens a full TCP connection. The port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with a RST packet, closing the connection before the handshake is completed.

SYN scans are not surreptitious enough; firewalls are in general (for wired network), scanning and blocking packets in the form of SYN packets are possible then FIN bit ON packets are able to pass through firewalls with no modification to its purpose. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand.

TABLE-VI
FEATURE EXTRACTION FROM TCP/IP HEADER

Feature	Description
F-1	Source Port
F-2	Destination Port
F-3	Connection Duration
F-4	Number of Packets
F-5	TTL (Time to Life)
F-6	ToS (Type of Service)
F-7	TCP Segment length
F-8	Reserved Flag Groups
F-9	URG- Flag
F-10	ACK- Flag
F-11	PSH – Flag
F-12	RST- Reset Flag
F-13	SYN- Flag
F-14	FIN- Flag
F-15	Window length group
F-16	TCP options Group
F-17	Data Length Group
F-18	TCP length Group
F-19	Start Hour

The Extracted features for TCP/IP header are trained with the help of Support Vector Machine, and accuracy of classification is used to test the given data, this is used for Lids and Gids for Anomaly detection engine (In this paper only TCP/IP header is considered for feature extraction for finding out the attacks initiated).

D. Support Vector Machine

SVM is used for solving a variety of learning, classification and prediction problems. Support vector machines (SVMs) are learning systems that use a hypothesis space of linear functions in a high-dimensional feature space, trained with a learning algorithm from optimization theory. This learning strategy, introduced by Vapnik et al. [21], is a very powerful method that has been applied in a wide variety of applications. The basic SVM deals with two-class problems—in which the data are separated by a hyper plane defined by a number of support vectors. Support vectors are a subset of training data used to define the boundary between the two classes. Kernel function plays an important role in SVM, in practice, various kernel functions can be used, such as linear, radial, polynomial or Sigmoidal as per the complexity of input data set.

E. Rule Pruning

For Rule pruning and Feature ranking, three performance criteria can be considered using SVM; Accuracy (A) of classification, Training Time (TT) & Testing Time (TST). Each feature can be ranked as "important (I)", "secondary(S)" and "useless (U)" for ids and above 19 features can be ranked according to the following rules to check the performance comparison of original 19 features.

Rule Set: (MukkaMala) [12]

1. **If** A↓ **and** TT↑ **and** TST↓ → I
2. **If** A↓ **and** TT↑ **and** TST↑ → **I**
3. **If** A↓ **and** TT↓ **and** TST↑ → **I**
4. **If** A ≈ **and** TT↑ **and** TST↑ → **I**
5. **If** A ≈ **and** TT↓ and TST↑ → **S**
6. **If** A ≈ **and** TT↑ **and** TST↓ → S
7. **If** A ≈ **and** TT↓ **and** TST↓ → **U**
8. **If** A↑ **and** TT↑ **and** TST ↓ → S
9. **If** A↑ **and** TT↓ **and** TST ↑ → S
10. **If** A↑ **and** TT↓ **and** TST ↑ → **U**

Important Feature {F-5, F-7, F-12, F-14}; Secondary Feature< F-3, F-10, F-11, F-13, F-19>; Useless (F-1, F-2, F-4, F-6, F-8, F-9, F-15, F-16, F-17, F-18)

IV. RESULTS AND VALIDATION

In this paper SVM $^{\text{LIGHT}}$ [23] is used for Training & Testing the Feature extracted from TCP/IP header for Anomaly detection and binary classification is used for detecting the Intruders activity classified in Table V. For Training & Testing (files used in this research can accessed from Appendix-A), Operating System UBUNTU 9.10 & P IV Dual core based machine is used. Audit data is firstly formatted into SVM $^{\text{LIGHT}}$ data format then applied for training and testing.

For Training data set

```
$ ./svm_learn data/train.txt     data/model.txt
```

For Classification

```
$ ./svm_classify data/test.txt      data/model.txt     data/prediction.txt
```

Table- VII
TRAINIG DATA SET

Input Feature	Train Data Set	Parameter (C,γ)	CPU Run Time (in Sec)	Mis Classified	Support Vector
9	476	Default	1.56	120	243
9	208	Default	0.85	52	108
6	482	Default	1300. 57	120	244
7	482	Default	2.19	120	244

Table-VIII
TEST DATA SET

Input Features	Test Data Set	Correct	Incorrect	Accuracy
9	476	356	120	(74.79/100)%
9	208	156	52	(75.00/100)%
6	482	362	120	(75.10/100)%
7	482	362	120	(75.10/100)%

Model file generated after training of training data set is confidence value generated by SVM $^{\text{LIGHT}}$, which is used to test the given test data set for prediction, Accuracy shows the True positive generated by detection engine. Accuracy generated above is on behalf of Default parameter of C& γ and linear function is used, the prediction file generated is a confidence file for testing data set on behalf of this prediction can be generated whether the node is an intruder or a normal node.

V. CONCLUSION & FUTURE WORK

In this model True positive will be reported very fast in Lids & Friend list generated by Lids will be sent to the Gids module for further investigation. Global Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes like routing, and deciding the cluster head for scalable adhoc networks. For detection engine machine learning algorithm Support Vector Machine is used which is light weighted and considered best among the supervised learning algorithms, prediction (accuracy) generated by the SVM $^{\text{LIGHT}}$ for different input features and different values of training and testing examples are satisfactory. Future work can be included that extraction of features from UDP & control packets for identifying the attacks possible in Adhoc network and to generate the model file and testing that model file in different scenarios and finally deploying the detection engine in node models for intrusion detection system.

REFERENCES

[1] Husain, S.; Gupta, S.C.; Chand, M.; Mandoria, H.L.; , "A proposed model for Intrusion Detection System for mobile adhoc network," *Computer and Communication Technology (ICCCT), 2010 International Conference on* , vol., no., pp. 99-102, 17-19 Sept. 2010, doi: 10.1109/ICCCT.2010.5640420
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5640420&isnumber=5640373

[2] Zhanfei Ma; Xuefeng Zheng; , "Cooperation modeling for intrusion detection system based on Multi-SoftMan," *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*, vol., no., pp.493-496, 20-22 Aug. 2009, doi: 10.1109/ICASID.2009.5276984
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5276984&isnumber=5276889

[3] Chengqi Song, Qian Zang,"Suppressing selfish behavior in adhoc networks with one more hop" 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, 2008, ISBN:978-963-9799-26-4 , published in Lecture Notes in Mobile Networks and Applications , Computer Science, vol - 14 Issue- 2, 01 April, 2009, Springer Netherlands, pp. 178-187, doi: 10.1007/s11036-008-0145-2
URL: http://dx.doi.org/10.1007/s11036-008-0145-2

[4] Otrok, H.; Debbabi, M.; Assi, C.; Bhattacharya, P.; , "A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks," *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference*, pp.86, 22-29 June 2007, doi:10.1109/ICDCSW.2007.91
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4279094&isnumber=4278984

[5] Huaizhi Li; Singhal, M.;, "A Secure Routing Protocol for Wireless Ad Hoc Networks," *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on* , vol.9, no., pp. 225a, 04-07 Jan. 2006,doi:10.1109/HICSS.2006.29
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579751&isnumber=33369

[6] Razak, S.A., Furnell, S., Clarke, N. Brooke, P. Mehrotra, Sharad. Zeng, Daniel, Chen, Hsinchun. Thuraisingham, Bhavani. "A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks--A Friend Approach", *Lecture Notes In Computer Science*, volume 3975, pp. 590-595, 2006, Springer Berlin / Heidelberg .doi: 10.1007/11760146_62
http://dx.doi.org/10.1007/11760146_62

[7] Abusalah, L.; Khokhar, A.; Guizani, M.; , "NIS01-4: Trust Aware Routing in Mobile Ad Hoc Networks," *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, vol., no., pp.1-5, Nov. 27 Dec.1, 2006, doi:10.1109/GLOCOM.2006.264;URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4150894&isnumber=4150630

[8] Balakrishnan, K.; Jing Deng; Varshney, V.K.; , "TWOACK: preventing selfishness in mobile ad hoc networks," *Wireless Communications and Networking Conference, 2005 IEEE* , vol.4, no., pp. 2137- 2142 Vol. 4, 13-17 March, 2005, doi: 10.1109/WCNC.2005.1424848
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1424848&isnumber=30731

[9] Hofmann, A.; Horeis, T.; Sick, B.;, "Feature selection for intrusion detection: an evolutionary wrapper approach," *Neural Networks, 2004. Proceedings. 2004 IEEE International Joint Conference on*, vol.2, no., pp. 1563 - 1568 vol.2, 25-29 July 2004,doi: 10.1109/IJCNN.2004.1380189
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1380189&isnumber=30097

[10] Nekkanti, R. K. and Lee C-W. "Trust Based Adaptive on Demand Ad hoc Routing Protocol" ACM-SE 42 Proceedings of the 42nd annual Southeast regional conference Huntsville, Alabama, , 2004, pp. 88-93
ISBN:1-58113-870-9, doi:10.1145/986537.986558
URL: http://portal.acm.org/citation.cfm?id=986558

[11] Pirzada, A. A and McDonald, C. "Establishing Trust in Pure Ad-Hoc Networks". In *Proceedings of the 27th Australasian Computer Science Conference (ACSC'04),* Dunedin, New Zealand, vol 26, pp. 47-54, 2004.
URL: http://portal.acm.org/citation.cfm?id=979929

[12] Andrew H. Sung, Srinivas Mukkamala, "Feature Selection for Intrusion Detection using Neural Networks and Support Vector Machines", Transport Research Record published by TRB Journal 2003,Issue number 1822, ISSN: 0361-1981, pp 33-39. URL: http://dx.doi.org/10.3141/1822-05

[13] Davis, J.; Hill, E.; Spradley, L.; Wright, M.; Scherer, W.; Zhang, Y.; , "Network security monitoring - intrusion detection," *Systems and Information Engineering Design Symposium, 2003 IEEE* , vol., no., pp. 241- 246, 24-25 April,2003,doi:10.1109/SIEDS.2003.158030
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1242425&isnumber=27841

[14] Yan, Z., Zhang, P. and Virtanen, T. "Trust Evaluation Based Security Solution in Ad Hoc Networks". In *Proceedings of the 7th Nordic Workshop on Secure IT Systems, NordSec 2003*, Gjovik, Norway, pp. 1-14, 2003.

[15] Eschenauer, L. "On Trust Establishment in Mobile Ad-Hoc Networks," Master's Thesis, *Department of Electrical and Computer Engineering*, University of Maryland, 2002.
URL: http://drum.lib.umd.edu/bitstream/1903/6336/1/MS_**2002**-10.pdf

[16] Bhargava, S.; Agrawal, D.P. , "Security enhancements in AODV protocol for wireless ad hoc networks ," *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th*, vol.4, no., pp.2143-2147 vol.4, 2001, doi: 10.1109/VTC.2001.957123
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=957123&isnumber=20686

[17] Jiejun Kong; Petros, Z.; Haiyun Luo; Songwu Lu; Lixia Zhang; , "Providing robust and ubiquitous security support for mobile ad-hoc networks," *Network Protocols, 2001. Ninth International Conference on*, vol., no., pp.251-260, 14 Nov. 2001, doi: 10.1109/ICNP.2001.992905
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=992905&isnumber=21404

[18] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (ACM MobiCom'00), Boston, MA, pp. 275-283, Aug. 2000. ISBN: 1-58113-197-6 doi: 10.1145/345910.345958
URL: http://portal.acm.org/citation.cfm?id=345958

[19] H. Debar, M. Dacier, and A.Wespi, "A Revised Taxonomy for Intrusion Detection Systems," *Annales of Telecommunications,* vol. 55, pp. 361-378, 01July,2000 Springer Paris ISSN- 0003-4347. doi: 10.1007/BF02994844
URL: http://www.springerlink.com/content/4xq65ng0l0801626/

[20] R. P. Lippmann and R. ***K.*** Cunningham. "Improving intrusion detection performance using keyword selection and **neural networks: *Computer Networks,*** The International Journal of Computer and Telecommunications Networking vol. 34, no. 4, pp. 597403, 2000. Elsevier North-Holland, Inc. New York, NY, USA, doi : 10.1016/S1389-1286(00)00140-7
URL: http://portal.acm.org/citation.cfm?id=361122

[21] Vapnik, V.N., "*The Nature of Statistical Learning Theory"*, 1st ed., Springer-Verlag, New York, 1995, series: Information Science & Statistics, ISBN: 978-0-387-98780-4

[22] J. Frank, ''Artificial intelligence and intrusion detection: Current and future directions," in ***Proceedings of the 17th National Computer Security Conference.*** Baltimore, MD, 1994.
URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.5769

[23] Joachims. Thorsten; "SVM ^{LIGHT}: Support Vector Machine",
URL: http://svmlight.joachims.org/

APPENDIX-A

Statistics used in simulation for Testing and Training of Support Vector Machine can be downloaded from URL given below password can be demanded from mail id mentioned at top.
URL: http://depositfiles.com/files/nwctbaspz