Journal of Engineering Science and Technology
Vol. 7, No. 5 (2012) 623 - 634

BLACK HOLE ATTACK IN AODV & FRIEND FEATURES[1] UNIQUE EXTRACTION TO DESIGN DETECTION ENGINE FOR INTRUSION DETECTION SYSTEM IN MOBILE ADHOC NETWORK

HUSAIN SHAHNAWAZ[1,2,*], GUPTA S.C.[3]

[1]Research Scholar Graphic Era University, Dehradun (U.K) India
[2]Department of Electrical Engineering Faculty of Engineering,
King Khalid University, Abha, KSA
[3]Indian Institute of Technology, Roorkee (U.K.) India
*Corresponding Author: shahnawaz.husain@hotmail.com

Abstract

Ad-hoc network is a collection of nodes that are capable to form dynamically 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 Mobile 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 (MANET) where security is a crucial issue and they are forced to rely on the neighbor node, trust plays an important role that could improve the number of successful data transmission. Larger the number of trusted nodes, higher successful data communication process rates could be expected. In this paper, Black Hole attack is applied in the network, statistics are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to find out the accuracy of detection engine by using support vector machine. In this paper True Positive generated by the detection engine is very high and this is a novel approach in the area of Mobile Adhoc Intrusion detection system.

Keywords: Black hole attack, Denial of service attack, Detection engine, Intrusion detection system, Friend features, Mobile Adhoc network.

1. 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

[1] Features are called as friend features because after detecting the intruders we are not punishing the node, we only foster the trusted nodes after applying the voting mechanism.

have legitimate access to the system but are abusing their privileges [1]. An intrusion detection system (IDS) dynamically monitors the system and user actions in the network in order to detect intruders. Because an information system can pursue from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system which is not susceptible to attacks. 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.

Research on IDSs began with a report by Anderson [2] followed by Denning's seminal paper [3], which lays the foundation for most of the current intrusion detection prototypes. Since then, many research efforts have been devoted to wired Intrusion Detection Systems. Numerous detection techniques and architecture for host machines and wired networks have been proposed. A good taxonomy of wired IDSs is presented in [4].

With the rapid proliferation of wireless networks and mobile computing applications, new vulnerabilities that do not exist in wired networks have appeared. Security poses a serious challenge in deploying wireless networks in reality. 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.

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. Once the node is compromised, intrusion prevention system will have little effect in protecting the network, in this situation, the role of intrusion detection is more important. 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. Type of attacks possible in Mobile Adhoc network is given in Table 1.

Table 1. List of UTC and APF.

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

In this paper black hole attack is applied in Mobile Adhoc Network, In black hole attack [5-7], a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants

to intercept. In this way attacker node will always have the availability in replying to the route request and thus attract the whole traffic of the network & intercept the data packet and further it may retain it or drop it.

2. 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. Otrok, et al. [8], Davis et al. [9], Yan et al. [10], and Kong et al. [11] have 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 [12] have extended the IDS model described in [13] to enhance the security in AODV (Ad-hoc on demand Distance Vector) routing protocol. Watchdog [14] 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. Kong et al. [11] follow the concept of [14] but work with ADOV. They add a next hop field in AODV packets so that a node can be aware of the correct next hop of its neighbors. They also considers more types of attacks, such as packet modification, packet duplication, and packet-jamming DoS attacks. Balakrishnan et al. [15] have proposed a way to detect packet dropping in ad-hoc networks. Trust features [10, 16-22] in existing trust-based routing schemes for MANET.

The model in [23] is derived from previous research provide evidence on how a friendship mechanism could be used to improve the accuracy of IDS in MANET [17]. This model is extended in [24] to design the attack possible using TCP protocol, right now it is not needed in Mobile Adhoc Network but only for the sake of future extensions and possibilities and in [25] intrusion detection system for Denial of service attack. Ibrahim [26] introduced a hierarchical off-line anomaly network intrusion detection system based on Distributed Time-Delay Artificial Neural Network is introduced. The results indicate that dynamic neural nets (Distributed Time-Delay Artificial Neural Network) can achieve a high detection rate, where the overall accuracy classification rate average is equal to 97.24%.

One of the main issues in MANET IDS is 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.

3. Proposed Frame Work

In [23] some assumptions that each node has a list of initial trust given in Table 2, 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 in Fig. 1. These initial lists are known as Direct Friend Mechanism (DFM). Description about

complete model like Gids (Fig 2.), Lids, node initial Trust, Indirect Trust, Feed-back Table can be accessed from [23].

Table 2. Node's Initial Trust.

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

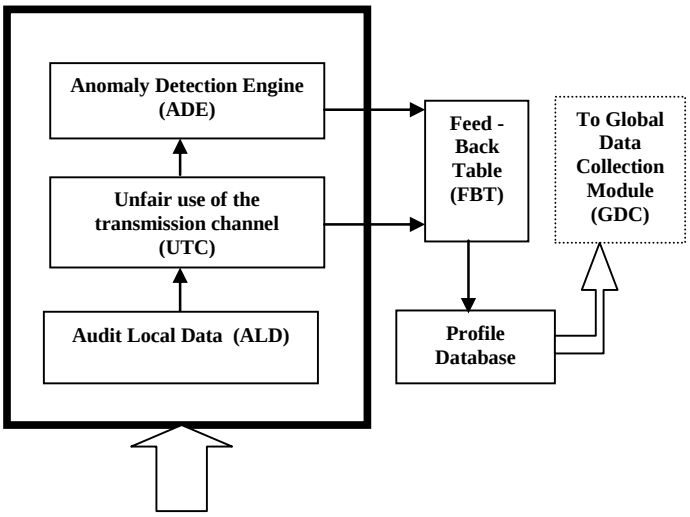

Fig. 1. Local Intrusion Detection System (Lids) [23].

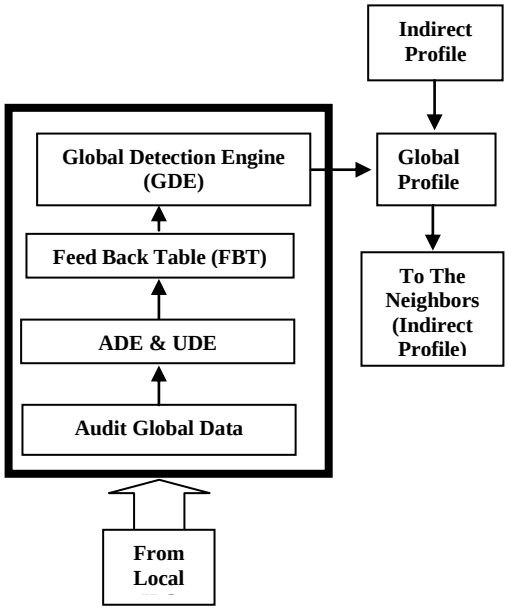

Fig. 2. Global Intrusion Detection System (Gids) [23].

3.1. 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)

And accuracy of the IDS system is based on above mentioned parameters.

Accuracy of the System = (TP+TN) / (TP+TN+FP+FN);

In [23], IDS model is divided into two sub-models one is Local IDS and another is Global IDS and they follow the 20:80 Rule to speed up their detection rate. In Lids the thresh hold values is set very high in the detection engine to detect the highly malicious node. Lids use Table 3 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) [23]. 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 3. Feed Back Table (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 4.

Table 4. 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

Feature Selection in the area of intrusion detection can be found in [27, 28], where standard feature selection techniques (forward / backward search, beam search or sequential search) are applied in combination with decision trees and keyword based IDS.

3.2. Simulation environment

Opnet Modeler is used for simulation; and Simulation Area is 1 Sq. Kilometer, there are 21 MANET workstations; with random mobility of (0-20) m/s, following a trajectory during simulation Trajectory 5 (a predefined trajectory in Opnet) shows in Fig. 3 as white lines , all nodes are AODV enabled, sending the Route Request for mobile node 20. Figure 3 shows the environment of simulation. Simulation parameters at a glance are given in Table 5. To apply Black Hole attack, AODV parameters for normal & malicious nodes are given in Table 6, MANET Traffic[2] generated parameters for normal and malicious nodes are given in Table 7.

Initially simulation is carried out without malicious node then one malicious node is inserted in the network in this environment node 5[3] is the malicious node and performance of the system is compared with and without malicious node.

Various features are generated after the simulation but few of them can be considered for further evaluation, which are used in Section 3.4. Performance evaluation of network without malicious node and with malicious node can be measured but they are not required in this paper because it is focused on designing of Intrusion detection system.

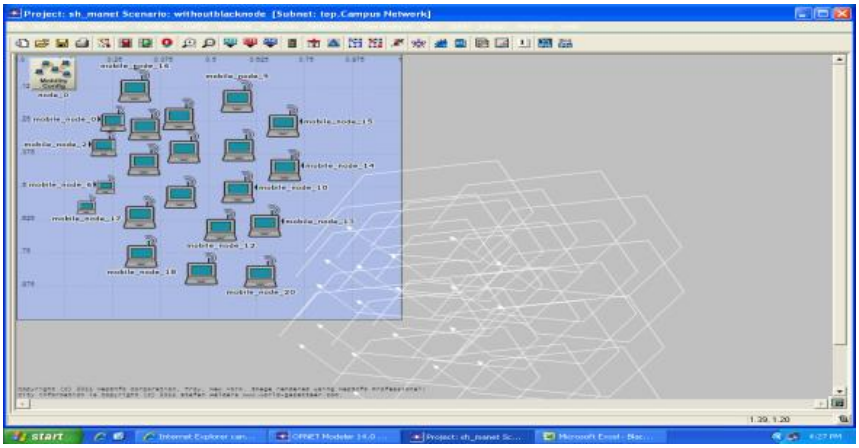

Fig. 3. Simulation Environment.

Table 5. Simulation Parameters at a Glance.

Parameters	Value
Simulation Area	1000*1000(in meters)
Simulation Time	3600 Sec
Nodes	21
Mobility	(0-20)m/sec (Random)
Distribution	Random
Trajectory	Trajectory-5
Routing Protocol	AODV

[2]It is called as MANET Traffic because in Mobile Adhoc Network in place of Application layer we have Manet Traffic Generation layer.

[3]we can insert more than one malicious node it will disturb the network but we are focused only to gather the statistics generated by the malicious node whether it is one or more than one it does not have impact on our aim.

Table 6. AODV Parameters for Malicious and Normal Node.

Parameters	Value (Normal Node)	Value (Malicious Node)
Route Discovery Parameters	Default	Custom Level
Route Request Retries	5	0
Route Request Rate Limit (Packets/Sec)	10	0
Gratutious Route Reply Flag	Enabled	Enabled
Destination only Flag	Enabled	Enabled
Acknowledgement Required	Enabled	Enabled
Active Route Timeout	3	3
Hello Interval	Uniform (1,1.1)	Uniform (1,1.1)
Net Diameter	35	1000
Timeout Buffer	2	0
TTL	Default	Default
Packet Queue Size (packets)	Infinity	0

Table 7. MANET Traffic Generation Parameters.

Parameters	Value (Normal Node)	Value (Malicious Node)
Start Time	10	10
Packet Inter Arrival Time	Exponential(1)	Exponential(1)
Packet Size	Exponential(1024) bits	Exponential(1024) bits
Destination IP Address	Mobile Node 20 (192.168.3.20)	Self (192.168.3.5)

3.3. Support vector machine

In this research SVM is used for solving learning, classification and prediction. 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 [29], 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.

3.4. Feature extraction

Following features [30, 31] can be extracted on behalf of above simulation for training and classification using SVM^{light} [32] for prediction and checking the accuracy of the system when black hole attack is applied. From the Simulation carried out in Section 3.3 visualized form is given in Figs. 4, 5 and 6 and statistics generated are exported to spreadsheet for analysis, audit data file generated using these features can be accessed from *Appendix A*.

- *Ratio of Routing Traffic Received (RRTR)* = (*Total Routing Traffic Received by malicious node / Total Routing Traffic Sent by complete N/W*)×100;
- *Ratio of Routing Traffic Sent* (*RRTS*) = (*Routing Traffic sent by Malicious Node / Routing Traffic Received by Malicious Node*)×100;
- *Ratio of Packet Drop* (*RPD*) = (*Packet Drop by Malicious Node / Total Packet Drop in N/W*)×100.

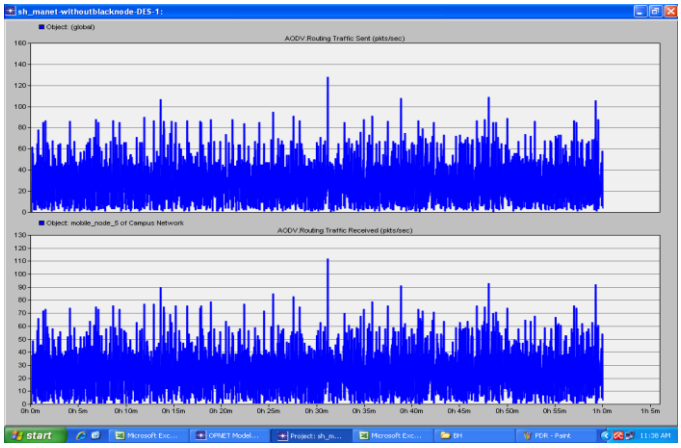

Fig. 4. Total Routing Traffic Sent by the Network and Routing Traffic Received by the Malicious Node.

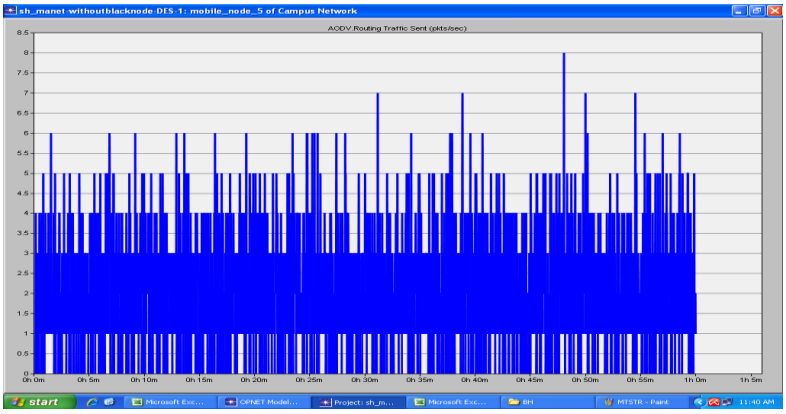

Fig. 5. Traffic Forwarded by Malicious Node.

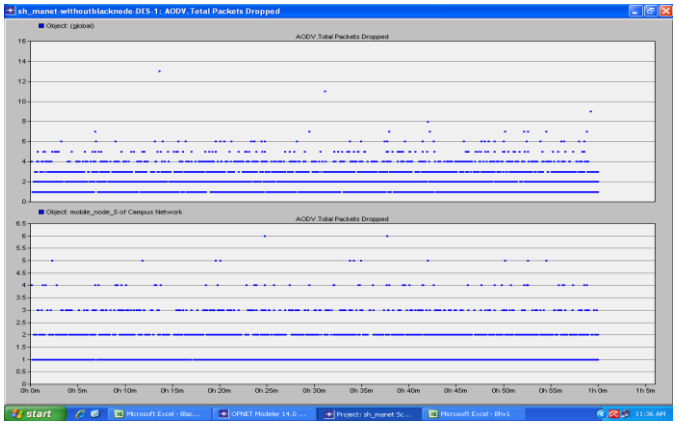

Fig. 6. Total Packet Drop by the Network and Packet Drop by the Malicious Node.

4. Results and Validation

From the simulation carried out in Section 3, it is cleared that in the presence of malicious node performance of the system degraded and overhead increases. Binary classification is used for detecting the Intruders activity for Black Hole attack. For Training & Testing, Operating System UBUNTU 9.10 & P IV Dual core based machine is used. Audit (Training & Testing) data is formatted into svm light data format before classification and testing.

For Training data set (commands used in training and testing)

$. /svm_learn –c <value> -g <value> <i/p file> <model file>

For Testing the testing data set

$. /svm_classify <test file> <model file> <prediction file>

Model file generated after training of training data set is confidence value generated by SVM ^{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 different values considered for C & γ parameters [29], and linear, radial & Sigmoidal functions are used. Tables 8 and 9 show the result of training and testing. The prediction file generated is a confidence file for testing data set on behalf of this we can predict whether the node is an intruder or a normal node. Model file generated is a detection engine which can be deployed in Intrusion detection system.

Table 8. Trainig Data Set.

Input Features	Train Data- Set	Function	Parameters (C,γ)	CPU Run Time (Sec)	Mis-Classified	Support Vector
3	3568	LINEAR	DEFAULT	153.27	92	273
3	3568	LINEAR	0.5,0.5	36.39	1248	14
3	3568	LINEAR	1.0,0.5	2.90	2321	15
3	3568	LINEAR	1.0,1.0	13.07	2321	15
3	3568	LINEAR	2.0,1.0	2.89	2321	14
3	3568	RADIAL	DEFAULT	2.36	56	938
3	3568	RADIAL	0.5,0.5	1.87	52	814
3	3568	RADIAL	1.0,0.5	2.17	39	792
3	3568	RADIAL	1.0,1.0	3.41	40	920
3	3568	RADIAL	2.0,1.0	2.67	37	900
3	3568	Sigmoidal	DEFAULT	1.44	1247	2494
3	3568	Sigmoidal	0.5,0.5	1.54	1247	2494
3	3568	Sigmoidal	1.0,0.5	1.36	1247	2494
3	3568	Sigmoidal	1.0,1.0	1.39	1247	2494
3	3568	Sigmoidal	2.0,1.0	1.47	1247	2494

Table 9. Test Data Set.

Input Features	Test Data Set	Correct	Incorrect	Accuracy	Precision/Recall
3	3568	3476	92	97.42	99.78%/96.25%
3	3568	2320	1248	65.02	65.05%/99.91%
3	3568	1247	2321	34.95	50%/0.09%
3	3568	1247	2321	34.95	50%/0.09%
3	3568	1247	2321	34.95	50%/0.09%
3	3568	3512	56	98.43	98.63%/98.97%
3	3568	3516	52	98.54	98.84%/98.92%
3	3568	3529	39	98.91	99.39%/98.92%
3	3568	3528	40	98.88	99.35%/98.92%
3	3568	3531	37	98.96	99.39%/99.0%
3	3568	2321	1247	65.05	65.05%/100%
3	3568	2321	1247	65.05	65.05%/100%
3	3568	2321	1247	65.05	65.05%/100%
3	3568	2321	1247	65.05	65.05%/100%
3	3568	2321	1247	65.05	65.05%/100%

5. Conclusions and Future Work

In this paper, 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. Feature extracted for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols. 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 for input features and different values of C & γ to stabilized the system for given training and testing data sets are satisfactory. We will use the model file generated by the function at which accuracy is higher for final deployment of the detection engine. Future work can be included to extract the features from routing & MANET Traffic parameters 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. Zhang, Y.; and Lee, W. (2000). Intrusion detection in Wireless Ad hoc Networks. *Proceedings of the* 6th *Annual International Conference on Mobile Computing and Networking*, 275-283.
2. Anderson, J.P. (1980). Computer security threat monitoring and surveillance. *Technical Report*, James P. Anderson Co., Fort Washington, Pa, 19034.
3. Denning, D.E.; (1987). An intrusion-detection Model. *IEEE Transactions on Software Engineering*, SE-13(2), 222- 232.
4. Debar, H.; Dacier, M.; and Wespi, A. (2000). A revised taxonomy for intrusion detection systems. *Annales des Telecommunications*, 55(7-8), 361-378.
5. Zhang, X.; Sekiya, Y.; and Wakahara, Y. (2009) Proposal of a method to detect black hole attack in MANET. *International Symposium on Autonomous Decentralized Systems ISADS*'09, 1-6.
6. Lu, S.; Li, L.; Lam, K.-Y.; and Jia, L. (2009). SAODV: A MANET routing protocol that can withstand black hole attack. *International Conference on Computational Intelligence and Security CIS* '09, 2, 421-425.
7. Medadian, M.; Yektaie, M.H.; and Rahmani, A.M. (2009). Combat with Black hole attack in AODV routing protocol in MANET. *First Asian Himalayas International Conference on Internet AH-ICI* 2009, 1-5.
8. Otrok, H.; Debbabi, M.; Assi, C.; and Bhattacharya, P. (2007). A cooperative approach for analyzing intrusions in Mobile Ad hoc Networks. *Proceedings of the* 27th International Conference Distributed Computing Systems Workshops ICDCSW'07, 86.
9. Davis, J.; Hill, E.; Spradley, L.; Wright, M.; Scherer, W.; and Zhang, Y. (2003). Network security monitoring - intrusion detection. *Systems and Information Engineering Design Symposium IEEE*, 241-246.

10. Yan, Z.; Zhang, P.; and Virtanen, T. (2003). Trust evaluation based security solution in Ad hoc networks. *Proceedings of the* 7th Nordic *Workshop on Secure IT Systems*, *NordSec* 2003, 1-14.
11. Kong, J.; Petros, Z.; Luo, H.; Lu, S.; and Zhang, L. (2001). Providing robust and ubiquitous security support for Mobile Ad-hoc Networks. *Ninth International Conference on Network Protocols*, 251-260.
12. Bhargava, S.; and Agrawal, D.P. (2001). Security enhancements in AODV protocol for wireless ad hoc networks. *Vehicular Technology Conference*, 2001. *VTC* 2001 *Fall*. *IEEE VTS* 54th, 4, 2143-2147.
13. Ma, Z.; and Zheng, X. (2009). Cooperation modeling for intrusion detection system based on Multi-SoftMan. *Proceedings of* 3rd *International Conference on Anti-counterfeiting, Security, and Identification in Communication ASID* 2009, 493-496.
14. Song, C.; and Zang, Q. (2009). OMH - Suppressing selfish behavior in Ad hoc Networks with one more hop. *Mobile Networks and Applications*, 14(2), 178-187.
15. Balakrishnan, K.; Deng, J.; and Varshney, V.K. (2005). TWOACK: preventing selfishness in Mobile Ad hoc Networks. *Wireless Communications and Networking Conference IEEE*, 4, 2137-2142
16. Li, H.; and Singhal, M. (2006). A secure routing protocol for Wireless Ad hoc Networks. *Proceedings of the* 39th *Annual Hawaii International Conference on System Sciences HICSS*'06, 9, 225a.
17. Razak, S.A.; Furnell, S.; Clarke, N.; and Brooke, P. (2006). A two-tier intrusion detection system for Mobile Ad hoc Networks - A friend approach. Springer Link, *Lecture Notes in Computer Science*, 3975, 590-595.
18. Abusalah, L.; Khokhar, A.; and Guizani, M. (2006). NIS01-4: Trust aware routing in Mobile Ad hoc Networks. *Global Telecommunications Conference GLOBECOM* '06 *IEEE*, 1-5.
19. Nekkanti, R.K.; and Lee C.-W. (2004). Trust based adaptive on demand Ad hoc routing protocol. *Proceedings of the* 42nd *ACM Southeast Regional Conference*, 88-93.
20. Pirzada, A.A.; and McDonald, C. (2004). Establishing trust in pure Ad-hoc networks. *In Proceedings of the* 27th *Australasian Computer Science Conference* ACSC'04, 26, 47-54.
21. Eschenauer, L. (2002). *On trust establishment in Mobile Ad hoc Networks*. Master's Thesis, Department of Electrical and Computer Engineering, University of Maryland, College Park.
22. Mohammed, Y.A.; and Abdullah, A.B. (2009). Security mechanism for MANETs. *Journal of Engineering Science and Technology* (*JESTEC*), 4(2), 231-242.
23. Shahnawaz, H.; Gupta, S.C.; Mukesh, C.; and Mandoria, H.L. (2010). A proposed model for intrusion detection system for Mobile Ad hoc Network. *Proceedings of* 2010 *International Conference on Computer and Communication Technology* (*ICCCT*), 99-102.
24. Shahnawaz, H.; and Gupta, S.C. (2011). Friend features extraction to design detection engine for intrusion detection system in Mobile Ad hoc Network.

International Journal of Computer Science & Information Technology, 2(4), 1569-1573.

25. Shahnawaz, H.; Gupta, S.C.; and Mukesh, C. (2011). Denial of service attack in AODV & friend features extraction to design detection engine for intrusion detection system in Mobile Ad hoc Network. *Proceedings of* 2011 2nd *International Conference on Computer and Communication Technology* (*ICCCT*), 292-297.
26. Ibrahim, L.M. (2010). Anomaly network intrusion detection based on distributed time-delay neural network (DTDNN). *Journal of Engineering Science and Technology* (*JESTEC*), 5(4), 457-471.
27. Lippmann, R.P.; and Cunningham, R.K. (2000). Improving intrusion detection performance using keyword selection and neural networks. *Computer Networks*: *The International Journal of Computer and Telecommunications Networking*, 34(4), 597-603.
28. Frank, J. (1994). Artificial intelligence and intrusion detection: Current and future directions. *Proceedings of the 17th National Computer Security Conference*, 10, 1-12.
29. Vapnik, V. (1995). The nature of statistical learning theory (Information Science & Statistics). (1st Ed.) Springer-Verlag, New York.
30. Hofmann, A.; Horeis, T.; and Sick, B. (2044). Feature selection for intrusion detection: An evolutionary wrapper approach. *Proceedings of the IEEE International Joint Conference on Neural Networks*, 2, 1563-1568.
31. Mukkamala, S.; and Sung, A.H. (2003). Feature selection for intrusion detection using neural networks and support vector machines. *Journal of the Transport Research Record*, 1822, 33-39.
32. Joachims, T. (2008). SVM^{light}: Support Vector Machine. URL: http://svmlight.joachims.org/.

Appendix- A

The supporting files (Training & Testing data set) generated after simulation and used for designing of detection engine can be requested from above mentioned email.