I.J. Modern Education and Computer Science, **2016, 7, 61-67**
Published Online July 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2016.07.07

Machine Learning Cross Layer Technique to Detect Sink Hole Attacks in MANET

Dr.G.Usha
Associate Professor, Karpagam College of Engineering,Coimbatore,India
Email: ushag2@gmail.com

Dr.K.Mahalakshmi
Associate Professor, Karpagam College of Engineering,Coimbatore,India
Email: prof.dr.mlk@gmail.com

Abstract—Adhoc networks uses mobile nodes to communicate among itself in which it does not have any fixed infrastructure like access point or base station. Due to dynamic network topology MANET security is a challenging task. Most of the routing protocols in MANET assumes a cooperative environment for communication. But, in the presence of malicious nodes, providing security to MANET is critical issue. Due to the increasing applications of MANET building an effective intrusion detection system are essential. This paper addresses using an intelligent approach for intrusion detection in MANET using cross layer technique. We show an paradigm of SVMs, FDAs and AIS approaches for intrusion detection in terms of classification accuracy.

Index Terms—AODV (Adhoc on demand distance vector routing), Cross Layer Security, Mobile adhoc networks, Security.

I. Introduction

Improving security in MANET is an essential task [1] [2].A MANET system is consisting of autonomous system of mobile nodes. Each node in MANET can act as router/gateways. Thus the MANET has unique characteristics compared to other conventional networks [3].Thus the MANET has dynamic topology, resource constrains and no physical infrastructure such as base station. MANET has widely used in military applications such as sharing information in battlefield, conferences, business meetings, emergency disaster relief after earthquake, hurricane, fire[4].Ubiquitous computing and pervasive computing are important era of current MANETs. Many authors have [5][6][7] proposed solutions for securing single layer. But single layer features are not enough to find the attacks completely. One can improve the detection ratio of attacks with the help of cross layer features [7][8].

Mobile adhoc networks suffer for various kinds of attacks such as black hole attack, gray hole attack, sinkhole attack, wormhole attacks. Typically the attacks can also be classified [9] as resource consumption attack, route invasion attacks, node isolation attacks, route disruption attacks. Sinkhole attack is a type of route disruption attacks in which the malicious nodes do not cooperate in routing process [10].Thus the attacking node invades the normal routing behavior. Hence identifying and detecting this type of attack is one of the most important and critical task. Detecting attacks can be classified as misuse detection and anomaly detection. We have proposed a hybrid intrusion detection scheme, which the IDS is trained with both normal behavior and attacking behavior. In our work we have proposed cross layer based intrusion detection technique. But most of the intrusion detection techniques [11][12][13]have considered only single layer attributes. Cross layer approach is way of achieving information sharing between the layers. Single layer techniques and layered architectures are suitable for wired networks. Sharing knowledge about layer state has proved for better optimization in wireless environment. The clear understanding about layered architecture is, they are independent in nature. But, in cross layer approach we are not completely eliminating the layered approach and not even integrating all layers. Instead we are correlating the features of between layers.

Cross layer based intrusion detection systems are getting more popular nowadays. Several intelligent techniques are used to build IDS. In this paper we propose a new architecture for MANET intrusion detection system called the mobile adhoc cross layer intrusion detection (MACLIDS) .This cross layer based intrusion detection system is able to successfully identify attacks using an data classification module(DC) which leverages classification algorithms such as support vector machine, fischer discriminant analysis and artificial immune system(AIs) in order to determine if an attack is occurring .Not only that we have also compared the classification accuracy of SVMs, FDA and AIS .We have reduced the feature set using apriori algorithm.

The remainder of this paper is organized as follows: Section 2 provides a literature review of security related issues in MANET; Section 3 presents vulnerability of AODV protocol. Section 4 presents the architecture and design of the proposed technique, Section 5 gives the simulation results and analysis of the proposed technique in multiple scenarios, and Section 6 provides conclusions and future work.

The remainder of this paper is organized as follows: Section 2 gives an effective method of skeleton extraction. Section 3 describes the two-round hierarchical matching for Chinese calligraphic retrieval. Section 4 presents the experiments and evaluation. Conclusion and future work are given in the final section.

II. Related Work

We have observed many of the existing literature works has mainly focused on protecting single layer either MAC layer or Routing or Physical layer. From all of these perspectives, researchers focused to identify anomaly detection and misuse detection. Further research work has been focused in the direction to differentiate between normal traffic and attack one. Now we present representative research from each perspective.

In [14] the authors proposed solution for anomaly detection using temporal activities of routing behavior in MANET. For detecting anomalies they have proposed a new algorithm. In [15] the authors proposed solution to detect both anomaly and misuse behavior in MANET. They have proposed an intrusion detection system (IDS) which detects packet drops or delays in the network. For that they have used the scheme which relays on time synchronization using GPS. In [16][17] many techniques have been proposed to identify various kinds of attacks. For detecting anomalies they have proposed a new algorithm. In [18], the authors proposed architecture for intrusion detection and prevention. They proposed intrusion detection based on agents. They used server agent, monitor agent, information agent, and address probing agents. In their work some agents are static and dynamic. They proposed an algorithm to detect attacks in MANET. In [19] the authors proposed distributed IDS for MANET. They used cluster head to monitor the activities of other nodes in the network. In [20] the authors proposed a rule based decentralized IDS in which some nodes act as monitor nodes and observes the traffic in the network. In [21] they proposed dynamic anomaly detection for AODV protocol using single layer technique. The authors used PCA for dimensionality reduction.

In literature many work has been done based on cross layer issue. In [22] the authors proposed physical media independence architecture. They defined a set of characteristics for each layer. Additionally they provided guard module in which it is used to monitor the system characteristics. They have done the modifications in operating system in order to implement cross layer concept. Interlayer signaling pipe [23] used the wireless extension header to store cross layer information. They used IP data packets to carry messages from physical layer to application layer. In [24] the authors separately used an Internet Control message protocol for propagating events from one layer to other layer. For this they used an icmp status message. Further a handle is implemented for this message. The inspirational idea for implementing cross layer security in adhoc network has been proposed in [25].The authors used Mobile man architecture. It has a core component known as network status, which is a repository for collecting information regarding all protocol layers. Each protocol layer interacts with this repository. Very little work has been done in literature using cross layer IDS methods. In [26] the authors proposed IDS architecture in which it uses physical, MAC and routing layer. In [27] also the authors proposed distributed intrusion detection architecture using cross layer features against MANET. Many recent works also suggest the vulnerabilities of the AODV protocol and the solution using single layer technique [28] [29] [30].

III. AODV Protocol and Vulnerabilities

Here first we discuss about working of AODV protocol in detail. Next we discuss its vulnerabilities to various kinds of attacks.

3.1 Overview of AODV protocol

Distance Vector routing protocol is based on the algorithm known as bellman ford algorithm which is known as single source shortest path algorithm. In Distance Vector routing, every router maintains a routing table (i.e. vector), in which it stores the distance information to all reachable destinations. A router exchanges distance information with its neighbors periodically to update its routing table. The distance can be calculated based on metrics such like hop number, queue length or delay. If multiple paths exist, the shortest one will be selected. AODV implements its routing from Distance Vector routing protocols. In AODV route discovery processes consist of two phases: route establishment, route maintenance. In Route establishment phase AODV protocol has the message set of Route request (RREQ), Route reply (RREP), and for link status monitoring (HELLO). When a node wants to participate in routing, it broadcast a RREQ message to the nodes. When the intermediate nodes get the RREQ message, the nodes update their routing tables in the direction of the source node. The RREQ message also contains the most recent sequence number which is 32-bit unsigned integer. When the destination node receives RREQ message it replies (Unicasts) RREP message to source node. When RREP propagates, all the intermediate nodes update their routing table about the sequence number. In Route maintenance phase, AODV has Route error (RERR).RERR Messages is used to broadcast for broken links. These messages are generated directly by a node or passed on when received from another node. In order to understand the vulnerability of AODV protocol, next section we discuss how AODV protocol is affected by sinking behavior.

3.2 Vulnerabilities of AODV protocol

According to [13] AODV protocol subjects against various kinds of attacks.

Route Disruption Attacks: Route Disruption attacks means breaking down an existing route or preventing a new route from being established.

Route Invasion Attacks: Route invasion attack means that an inside attacker adds itself into a route between two nodes of a communication channel.

Resource Consumption Attack: Resource consumption attack refers to consuming the communication bandwidth in the network or storage space at individual nodes.

The attacker tries to misuse RREQ and RREP messages by dropping, modifying, or alternating the message headers. For example the message field of RREQ has the types RREQID, hop count, destination ip address, destination sequence number, source IP address, source sequence number, and flags. The attacker can modify the message type, increase or decrease the RREQ ID, replace the destination ip address with other address and so on. Likewise the attacker can also modify or change the RREP messages. Hence it is a critical issue to handle these attacks.

3.3 Sink Hole Attack in Detail

Sink hole attacks are difficult to find because of following reasons. When the normal communication takes place in MANET, the sinking node tries to attract the neighboring nodes in various ways. In AODV protocol it either alters the data packets or drops the packets silently. One can wonder how it happens; the malicious node increases its sequence number. As we discussed above, the sequence number in AODV is used to intimate about the freshness of the route. The malicious node overhears the communication channel as a part and observes the sequence number of all nodes. After that it assigns itself as having the highest sequence number among all the nodes in the route and invades the channel abruptly and drops the packets. For example in the following Fig1. Node 1 is source node and node5 is the destination.

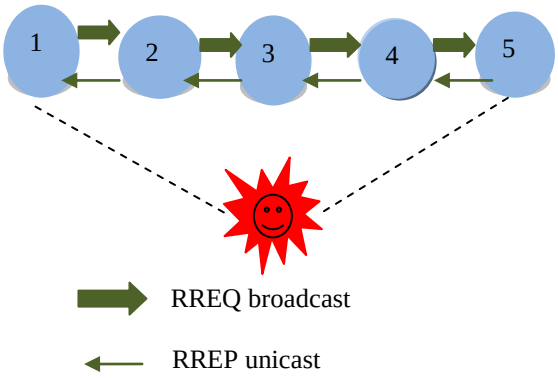

Fig.1.Sink hole attack in MANET

Initially, node 1 wants to send information to node 5 by broadcasting the RREQ message. Node 2 checks whether if it is the destination node. Since it is not the destination node it simply forwards the packet. Likewise the information propagates and finally reaches the destination node 5; hence communication takes place among the nodes. But when the invader or malicious node invades the network, the communication breaks. For example the malicious node overhears the network and updates its sequence number and sets its sequence number as the highest sequence number among all the nodes and broadcast it to others. The other nodes in the communication path also update this value in their routing table. This is the way in which the malicious node attracts other nodes. Thus the malicious node simply drops all the packets which come into it. This is the way the sinkhole attack takes place in this MANET.

IV. Proposed System Architecture

The following Fig 2 illustrates the proposed system architecture.

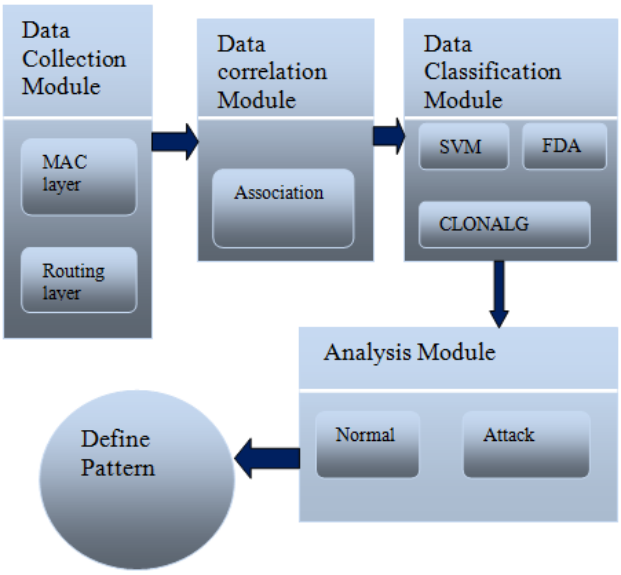

Fig.2. Proposed System Architecture

4.1 Data Collection Module

Data collection module is responsible for collecting data from MAC layer and Routing layer. A partial list of data collection attributes from these two layer is shown below.

Mac Layer	Network Layer
Retransmission of packets Delay between data and transmission Time delay between data and acknowledgement	Number of forwarded RREQ messages Number of dropped RREP messages Number of RERR messages

In our proposed IDS, hybrid intrusion detection technique is used. i.e., Data collection module consists of both normal and misuse data's.

4.2 Data Correlation Module

The proposed IDS is designed by combining intelligent modules as shown in Figure 2.The data correlation module correlates the data's between MAC layer and routing layer. We have used apriori algorithm because it

uses the principle if an item set is frequent then all its subsets or supersets must also be frequent. So apriori algorithm uses the value of the support measure as

$$\forall X, Y : (X \subseteq Y) \Rightarrow s(X) \geq s(Y)$$

Support of an item set never exceeds support of its subsets.

We are using Apriori algorithm because it uses the concept of pruning, hence it is efficient. This algorithm is efficient because it uses breadth-first search and a hash tree structure is used to reduce number of comparisons, i.e, instead of matching each transaction against every candidate this algorithm uses the concept of hashed bucket to match the candidate value. The main algorithm for frequent item set generation is described as follows:

1. From the data set find the frequent item set which is denoted as L k-1. L_k is the frequent item set of size k
2. In join step Ck is generated by joining L_{k-1} with itself i.e., using Cartesian product L_{k-1} x L_{k-1}.
3. In Prune step (apriori property): Any (k − 1) size item set that is not frequent cannot be a subset of a frequent k size item set, hence should be removed
4. Support count is obtained during frequent set L_k has been achieved.

The dataset which contains the value of MAC layer and routing layer can be joined and pruned as shown in steps 2 and 3.

4.3 Data Classification Module

SVM for Classification

Machine learning classification has been widely used to categorize data in to distinct classes. A model is first created based on the previous data which is known as training samples. Then this model is used to classify new data which is unseen samples. So Classification is essential for finding the best boundary between classes. Initially label the training data

$$\{\mathbf{x}_i, y_i\}, \ i = 1, \cdots, l, \ y_i \in \{-1, 1\}, \ \mathbf{x}_i \in \mathbb{R}^d$$

x which lie on the hyper plane'**s** is normal to hyper plane, |b|/||**w**|| is the perpendicular distance from hyper plane to origin. Now we can define two support hyper planes as

H1:$\mathbf{w}^T\mathbf{x}$ = b +δ
H2:$\mathbf{w}^T\mathbf{x}$ = b –δ

Map data to high dimensional space where it can easily classify with linear decision function. In order to achieve this we have to find a kernel function Φ(x) to map to different space. Φ is a mapping function.

Since the training algorithm only depend on data thru dot products. We can use a "kernel function" K such that

In our technique we are using radial based function (RBF).A RBF is a real-valued function whose value depends only on the distance from the origin, so that Φ(x)= Φ(||x||) .In order to give penalty to error term the cost can be defined as

$$\text{Cost} = C\left(\sum_i \xi_i\right)^k$$

Clonal Selection Algorithm for Classification

Clonal selection algorithms are based on immune system. The immune systems are summarized as distinguish between itself and non-self. Immune response system poses the following elements

Specificity: This element identifies and discriminates between different entities.

Adaptiveness: The element identifies new unseen entities that never existed previously.

Discriminate between self and non-self: This element is responsible for identifying the difference between self and non-self elements.

Memory: In memory the system recalls previous contact with foreign molecules and responds.

The clonal selection algorithm is said to be inspired by the following elements of the clonal selection theory Maintenance of a specific memory set Selection and cloning of most stimulated antibodies Death of non-stimulated antibodies Affinity maturation (mutation) Re-selection of clones proportional to affinity with antigen Generation and maintenance of diversity

4.4 Analysis Module

Based on the classification applied on the dataset the given input is classified as normal data and attack data. In this way the proposed technique detects the attack data.

V. Simulation Results

In the real time MANET environment the packet transmission is continuous. This is simplified in our simulation as it is repeated with different parameters. During every time of simulation the record sample is randomly abstracted from the test dataset and the classification occur. The detection procedure occurs as shown in Fig 3. We have used Ns-2 for simulation environment.Table1 illustrates the list of parameters used for simulation. In order to achieve a better comparison of the algorithms, we have calculated the overall false positive ratio(FPR),false negative ratio(FNR),true positive ratio(TPR),true negative ratio(TNR) are evaluated for CLIDS by evaluating the whole dataset.TPR values evaluates the cases where the intrusions or normal network behavior is correctly identified.TNR values are evaluated by correctly rejecting the malicious behaviour.FPR values are evaluated by where the normal communications are evaluated as attacks and FNR are evaluated as incorrectly rejecting the behavior of normal or attack data's. With the help of these values we have calculated overall accuracy of the system. Accuracy is calculated using the following formula,

Accuracy (%) = (TPR+TNR)/ (TPR+TNR+FPR+FNR)

TPR is known as true positive, TNR is known as true negative, FPR is known as false positive, FNR is known as false negative.

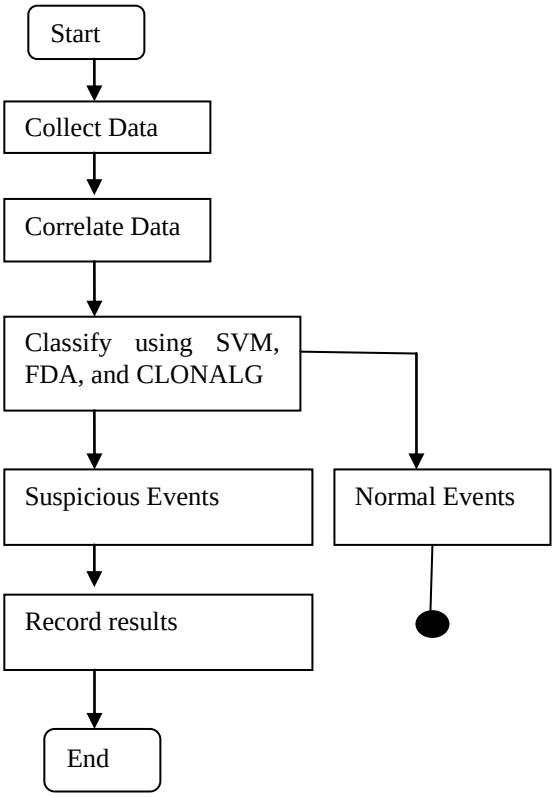

Fig.3. Detection Procedure for Evaluation

By using the accuracy formula we have calculated the accuracy of the algorithm as shown below. From the table 2 we have observed that cross layer SVM algorithm performs better than other algorithms.Fig 4 presents the simulation results and comparison of the above technique.

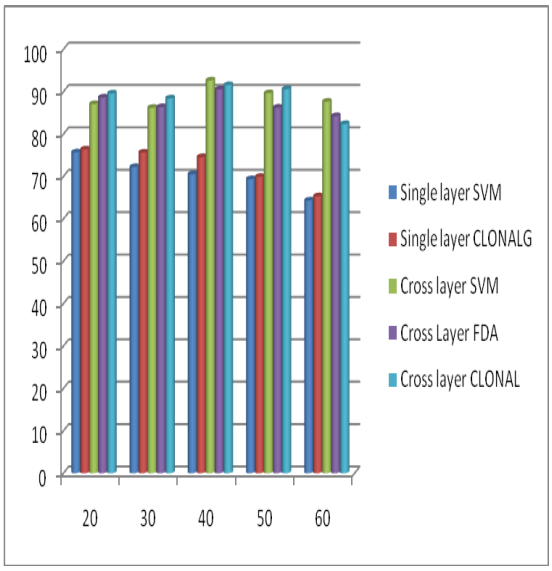

Fig.4. Comparison of the single layer technique with cross layer technique

Table 1. Simulation Environment

Property	*Value*	*Description*
Channel type	Wireless Channel	Channel Used
Propagation Model	Two ray ground	The radio propagation model used
Antenna type	Omni Antenna	Type of Antenna
Interface Queue type	Drop Tail/PriQueue	Queue used
MAC Type	802.11	MAC layer Protocol used
Maximum Packets in Queue	50	Packets in Queue
Topological Area	600m X 600 m	Area of simulation
Mobility Scenario	10 m/s	Node's mobility
Pause time	20 Sec	Node's pause time at simulation
Mobility Model	Random way point	For mobility of nodes

From Fig 3 it is observed that compared to single layer technique cross layer technique improves the performance of the network.

Table 2. Accuracy Calculation Table

Nodes	Single Layer SVM	Single Layer CLONALG	Cross Layer SVM	Cross Layer FDA	Cross Layer CLONAL
20	75.67	76.36	87.07	88.63	89.57
30	72.21	75.63	86.2	86.36	88.41
40	70.52	74.56	92.65	90.52	91.56
50	69.36	69.9	89.65	86.23	90.58
60	64.32	65.32	87.65	84.23	82.36

VI. Conclusion

This paper proposes a new architecture, MACLIDS, in order to improve the security of MANET. We have used SVM, and FDA and AIS algorithms to improve classification accuracy. We have proved the effectiveness of the new model for improving detection accuracy, which is demonstrated through multiple simulations.

We have used three classifiers for evaluating the detection accuracy of our proposed architecture. Some other classifiers may also be able to achieve better performance's in our future work we will use some existing classifier for our problem. Likewise, we can determine the most effective classifiers. Hence we can develop different intrusion detection system with

different classification techniques. We have considered only the sinkhole attack, not only that we have focused only on AODV protocol. Though AODV is on-demand routing protocol we will consider other routing protocol for additional type of attacks to further improve the accuracy of the overall system. Our future work will focus on more intelligent intrusion detection and prevention schemes in MANETs.

REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei,"A Survey on Attacks and Countermeasures in Mobile Ad Hoc Net-works",Wireless/Mobile network Security,2006 Springer.

[2] Nikola Milanovic,Miroslaw Malek,Anthony Davidson,Veljko Milutinovic,"Routing and Security in Mobile Ad Hoc Net-works", Published by the IEEE Computer Society,2004 .

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, pp. 38-47, 2004.

[4] C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.

[5] Kimaya Sanzgiri, Bridget Dahilly,"A Secure Routing Protocol for Ad Hoc Networks", IEEE International Conference on Network Protocols (ICNP'02), Page(s): 78 - 87, 2002.

[6] JamesParker, JeffreyUndercoffer, John inkston, Anupam Joshi,"On intrusion detection and response for mobile adhoc networks", IEEE International Conference on Performance, Computing and Communications, Page(s):747-752, 2004.

[7] Husain. Shahnawaz, Dr.S.C.Gupta, Chand.Mukesh, Dr. H.L.Mandoria,"A Proposed Model for Intrusion Detection System for Mobile Adhoc Network", IEEE conf on Computer & Communication Technology (ICCCT'10), Page(s): 99 - 102, 2010.

[8] Christoforos Panos, Christos Xenakis and Ioannis Stavraka-kis,"A novel intrusion detection system for manets", Springer .page(s).125-145, 2004

[9] Vijay T.Rasinghani,Sridhar Iyer,"Cross-layer design optimizations in wireless protocol stacks",SCienceDirect,Volume 27,Issue 8,Page(s):720-224,2003

[10] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," in Proc. 4th Annu. IEEEInf. Assurance Workshop, Page(s):60-67, 2003.

[11] Imad Aad, Jean-Pierre Hubaux, Edward W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM transactions on networking, Vol.16, no.4, 2008.

[12] Adnan Nadeem,Michael Howarth,"A Generalized Intrusion Detection & Prevention Mechanism for Securing MA-NETs",IEEE Proceedings on Ultra Modern Telecommunications & Workshops(ICUMT'09),Page(s): 1- 6 ,2009.

[13] Hidehisa Nakayama,Satoshi Kurosawa,Abbas Jamali-pour,Yoshiaki Nemoto,and Nei Kato,"A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Net-works",IEEE transactions on vehicular technology,vol.58,No.5, Page(s): 2471- 2481,2009.

[14] Haitao Liu; Rajiv Gupta,"Temporal Analysis of Routing Activity for Anomaly Detection in Ad hoc Networks", IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), 2006, Page(s): 505 - 508, 2006.

[15] S.Madhavi,"An Intrusion detection system in mobile adhoc networks"IEEE International Conference on Information Security and Assurance, 2008.

[16] P.Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communication and Multimedia, Page(s): 107–121, 2002

[17] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in GLOBECOM 2003 - IEEE Global Telecommunications Conference,vol. 22, no. 1, Dec 2003,Page(s): 2957 – 2961.

[18] Sampathkumar Veeraraghavan', S. Bose, K. Anand and A. Kannan,"An Intelligent Agent Based Approach for Intrusion Detection and Prevention in Adhoc Networks", IEEE International conference on ICSCN 2007, Page(s):534-536, 2007.

[19] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," in HICSS '03: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2. Washington, DC, USA: IEEE Computer Society, 2003.

[20] A. Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H.Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," in Proceedings of Intl.

[21] Workshop on Quality of Service and Security in Wireless and Mobile Networks, Page(s): 16–23, 2005.

[22] Hidehisa Nakayama,Satoshi Kurosawa,Yoshiaki Nemoto and Nei Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks",IEEE Transaction on vehicular technology,Vol.58,No.5,June 2009.

[23] Jon Inouye, Jim Binkley, and Jonathan Walpole. "Dynamic Network Reconfiguration Support for Mobile Computers", In ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Budapest, Hungary, September 26 – 30, 1997.

[24] Gang Wu, Yong Bai, Jie Lai, and A. Ogielski., Interactions between TCP and RLP in Wireless Interne". In IEEE GLOBECOM, volume 1B, pages 661–666, Rio de Janeiro, Brazil, December 1999.

[25] P. Sudame and B. R. Badrinath. On Providing Support for Protocol Adaptation in Mobile Networks.ACM/Kluwer special issue on wireless internet and intranet access. Published in Journal of Mobile Networks and Applications, Page(s):43–55, 2001.

[26] Conti, M.; Maselli, G.; Turi, G.; Giordano, S.Cross-layering in mobile ad hoc network design, Computer Volume: 37, Issue: 2, Digital Object Identifier 10.1109/MC.2004.1266295,Publication Year: 2004, Pages: 48 – 51 cited by: 39 IEEE/ACM Journals Computer Achieve.

[27] Thamilarasu, G., et al. A cross-layer based intrusion detection approach for wireless ad hoc networks. in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. 2005.

[28] Liu, Y., Y. Li, and H. Man. Short Paper: A distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks. in Security and Privacy for Emerging Areas in Communications Networks, 2005.

[29] Patel, M, Sharma, S ,"Detection of Malicious Attack in MANET a Behavioural Approach", Proc. IEEE third International conference on Advance Computing, pp.388-393,2013.

[30] Indirani, and K. Selvakumar, "A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)",International Journal of Parallel, Emergent and Distributed Systems, Vol. 29,no.1,pp.90-103, Apr 2014.

Autbors' Profiles

Dr.G.Usha completed her PhD in Anna University Chennai. Currently she is working as Associate Professor in Karpagam College of Engineering Coimbatore. She obtained her PG from Anna University Chennai. She completed her UG in Anna University Chennai. She is a GATE scorer .She had seven year of working experience in Anna University Chennai. Her area of research includes wireless security, Artificial Intelligence, Game theory, Graph theory and so on.

Prof Dr.K.Mahalakshmi, completed her PhD in Anna University Chennai in the year 2014. Currently she is working as a Professor in Karpagam College of Engineering Coimbatore. She obtained her PG from Allahabad University in the year 2004. She also holds another Masters degree in Business Application from Annamalai University in the year 2002. She has obtained her Bachelor of Engineering in Computer Science and Engineering from Annamalai University in the year 1996. She is a life time member if ISTE, and CSI member. She has eighteen year of teaching experience in various universities.

How to cite this paper: G.Usha, K.Mahalakshmi,"Machine Learning Cross Layer Technique to Detect Sink Hole Attacks in MANET", International Journal of Modern Education and Computer Science(IJMECS), Vol.8, No.7, pp.61-67, 2016.DOI: 10.5815/ijmecs.2016.07.07

