Volume-7,Issue-4, (Apr-17)
ISSN (O) :- 2349-3585

A Cloud FCM based intrusion detection model in a MANET environment

J. Samuel Manoharan[1], P. Muralidharan[2],G. Jayaseelan[3]
[1]Professor,[2]Asst. Professor, Dept. of ECE, Bharathiyar college of Engineering and Technology, Karaikal

Abstract— With the advent of ad-hoc networks, there has been a great boost in communication methodologies in the wireless domain. Numerous research contributions have been made especially in the case of mobile nodes or mobile ad hoc networks (MANET). The advantage of MANETs are that they don't require a predefined infrastructure like a router link, hub etc., The nodes in a MANET are capable of forming a network which is time dependant and not permanent to establish communication on the allocated path. An important parameter in design and implementation of MANET is security from attacks which may be internal or external which defines the efficiency of the MANET structure to a great extent. Routing attacks cause massive damage to MANETS and research contributions in the past have presented dedicated intrusion detection mechanisms to detect these attacks and consequently eliminate the malicious nodes from the network. The proposed work in this research paper addresses an efficient fuzzy clustering based algorithm for intrusion detection in a MANET implemented for a cloud storage environment. An important aspect of nodes in a MANET is that they need to be quite cooperative as they depend on every other node for transfer of information packets. This paper has presented a model and experimental justifications to improve the efficiency of the algorithm by minimizing the number of false detections of intrusions.

Keywords— Cloud storage, Intrusion detection systems, MANET, Fuzzy clustering techniques.

I. INTRODUCTION

With advancements in state of the art communication technologies and protocols, the field of information technology has undergone a great revolution especially in the area of handling large volumes of data and their storage in a cloud environment. This has become a great necessity especially with all communication and transactions going digital in today's environment. Promotions in business in the IT sector on a global scale greatly depend on cloud environment and its effective management. Efficiency of cloud depends greatly on systematic storage and fast retrieval in times of requirement. Another critical requirement of cloud is that it requires a fool proof secured environment to prevent theft or unauthorized access for manipulation of data. Security in clouds are greatly influenced by attacks termed as Intrusions which take many forms with each one causing massive damage in corresponding layers in the transport and application layers. Hence there is a great need for development of intrusion detection schemes or algorithms to improve the security of cloud storage systems. Since cloud storage environments do not require any infrastructure that is predefined, they are modeled using ad hoc networks preferably Mobile ad hoc networks (MANETS) with nodes in the network playing a major role in communication of information packets from source to destination. A typical cloud storage environment is depicted in figure 1

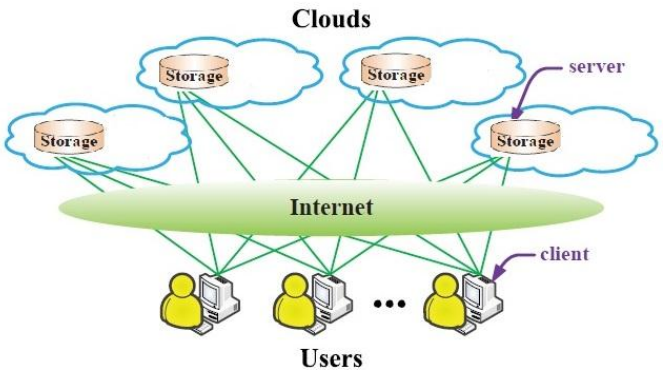

Figure 1. Illustration of Cloud environment

The efficiency in the cloud environment created as shown in figure 1 depends on several attributes such as protection of data and its authorization mechanism, secured channels for communication from source to destination, protection of nodes from unauthorized access and usage, effective intrusion detection mechanism to protect the nodes or if infected, a

mechanism to isolate the malicious node from the rest. A basic advantage of going in for cloud based storage over conventional storage mechanisms is that the data could be made available at any time and at any place where internet access is available. It eliminates the disadvantage of carrying the storage device to all places of mobility. The users in the large pool of data could be made available on demand the resources in the network. Prominent cloud infrastructures could be found in application engines of Google, Amazon, Microsoft Azure etc., As mentioned in previous sections, Mobile Ad hoc Networks (MANET's) are analogous to cloud computing networks for the proposed application in this paper. Cloud does not require any predefined infrastructure similar to mobile ad hoc networks. The intrusion detection and management systems proposed in this paper are implemented in the MANET architecture. A basic MANET architecture is depicted in figure 2.

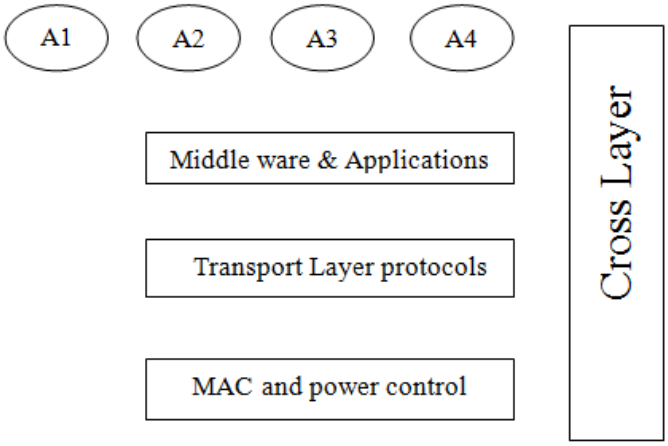

Figure 2. MANET architecture for communication for four users

As already known, MANET is a self organizing, self configuring capable of bringing together mobile nodes without wires and hence making it an infrastructure-less implementation. A MANET initiates the transfer of information in the form of packets from source to destination. Each node in the MANET has to make sure that it is configured perfectly to initiate the forwarding the packets to the next node. While they are characterized by numerous merits, MANET implementations are constrained by changing configurations as the nodes are mobile and also each of the nodes in the network have limited power and memory management capacities. The architecture as shown in figure 2 has three major layers namely the middleware and application layers, transport protocol layer and the control layer. The control layer is basically a technology enabling layer categorized into Local area (LAN), Metropolitan (MAN) and Wide area (WAN) networks. There is another category known as the personal area network or PAN which is active up to a distance of 8 - 11m. Variations in LAN include the Wireless LAN active from 1000 – 1700m. The next layer is the Networking layer which is responsible for defining the protocols required for self organizing, self configuring. One hop and multi-hop strategies for effective and fast node to node transport are also defined in this layer. The final layer is the middle layer concerned with group communication, memory allocation and sharing. MANETs incorporate almost all of state of art technologies like Blue tooth, WIMAX, IEEE 802.11 and Hyper LAN.

II.RELATED WORK

A number of research contributions have been found in the survey with a great boom in development of wireless communication technologies and protocols. Since the proposed work focuses on development of intrusion detection mechanism for a MANET in a cloud environment, the literature survey has been limited to contributions in IDS and security issues. The works of Bhosale et al has presented a review on the different types of intrusions, nature of attacks and the evident responses that could be seen from the nodes. The paper has presented a routing misbehavior attack in which attackers make use of the basic MANET concept that perfect cooperation is assumed between nodes in the network. A watchdog IDS technique has been presented in the paper from the works of Marti et al where the influence of the attack is reduced to a minimum amount by enhancing the throughput through the channel even in presence of the malicious node. Watchdogs observe the nodes for any deviation from normal behaviors and study the hop of the data from node to the next for detecting misbehavior. However, findings suggest that watchdog IDS fails in presence of false alarms, collisions and data drops. Findings from the research indicate that the above mentioned drawbacks have been effectively dealt with by utilizing an acknowledgement scheme IDS [4] [9]. An improvement in the above scheme has been brought about by

ISSN:-2349-3585 |www.ijrdt.org

adaptive acknowledgement technique proposed by Sheltami et al [7]. An intrusion detection scheme presented in the review works of [11] [14] [21] utilize a digital signature based technique to address the data drop and false alarm issues found in previous works. This is achieved by assuming that the malicious node is in between the source and destination and acting as intermediate nodes. These intermediate nodes which are malicious drop off the packets before passing them on to the next node and intimate this to the source through a forging acknowledgement. A transmission is said to be successful if the source receives the acknowledgement signal from the destination within a threshold time or declared unsuccessful on the other condition. Survey also indicates development of IDS techniques which are either network dependent or host dependent [24] [27]. Network based techniques have a network interface with a management console while the latter is software monitored. Research papers have also dealt with knowledge based techniques where events are recorded in database and intimated to the control while a similar event occurs in the future. On the other hand, behavior based IDS methods [3] generate an alarm to the console manager if any deviation from the normal behavior of the network is observed. Literature presents recent techniques like IDSX where X stands for extended to address Phantom intrusions and elimination of the intrusion in a minimum period of time [8]. The other prominent techniques found in the literature include Honesty Colloborative IDS [12] and neural network based techniques [7] [19]. Neural network based methods utilize watermarking techniques for IDS and SOM based hybrid techniques are also shown to produce high efficiency in throughput even in presence of intrusions. Another well known technique is the SCAN algorithm [15] where every node in the network scans or monitors every other node in its neighborhood for any malicious behavior. Results indicate 94% accuracy in identification of misbehaving nodes. In SCAN based methods, the misbehaving node is isolated by depriving it the access to the network. Other techniques for efficient IDS implementation include a multi agent system IDS known as MASID [6] [13] where a collection of predefined agents perform the function of detecting abnormal behavior. In a special case, where sufficient justifications are not available for proving a malicious behavior, the local agents combine in a cooperative manner to justify the abnormal behavior by providing additional information. Other techniques reported in the literature [10] include OCEAN where the state of the node is maintained and controlled by the neighbor node, CNMR [19] [24] which emphasizes on coordinated monitoring of node activity and the well known SOM based IDS whose backbone lie on the artificial neural network architectures. The works of Bo Sun et al present a Zone based approach for IDS where the node is identified as a gateway node if a node is physically connected to another node in a different zone. Internally connected nodes are known as Intra zonal nodes. Since the entire framework is divided into zones, the IDS computation time and hence the cost gets greatly reduced. The other issues addressed in the literature include security in the management console [25] [29]. Unlike tradition wireless networks where mobile devices connect through an access point, ad hoc networks which are the fopucs of study do not have such access points and hence form an architecture which is completely distributed in nature. This consequently affects the defense mechanism of the network to classify the nodes as trusted and non-trusted. Since the nodes are mobile in MANET, they are at liberty to join or leave the network at their own free will with or without prior notice causing in continuous change in network configurations. An additional problem related to compromised nodes [24] [31] is the potential Byzantine failures encountered within MANET routing protocols. A Byzantine failure is one in which direct observation of faulty nodes or behavior of them could never be achieved. The nodes arising from these kinds of failure inflict new routing messages causing deviation in the network transmission process. Based on the above findings, a fuzzy based clustering algorithm has been proposed in this paper where the inputs are converted into crisp sets to make a decision on the classification of trusted and non-trusted nodes.

III.PROPOSED WORK

A basic pseudo-code of intrusion detection mechanism and the algorithm for detection is illustrated below starting from the client and destination with knowledge of the different types of intrusions given to the database during recognition.

ISSN:-2349-3585 |www.ijrdt.org

Input: $y \in R^m$ *and* $\emptyset \in R^{mxn}$
Output: $\hat{x} \in R^n$ *and* $y = \emptyset\, \hat{x}$
$x^0 \leftarrow 0; r^0 \leftarrow y$
While halting condition is false do
$k \leftarrow k + 1$
$g^k \leftarrow \emptyset^T r^{(k-1)}$
$\lambda^k \leftarrow arg\ max\ |g^k|$
If cut (A,B) $= \sum_{u \in A, v \in B} w(u, v)$
$d_k \leftarrow \emptyset^T (y - \emptyset^T x^{k-1})$
else
$g_k \leftarrow \emptyset^T (y - \emptyset^T x^{k-1})$
endif
$\hat{x} = x^k$
Return $\hat{x}$

The functional architecture of the proposed solution is based on Google App Engine (GAE) platform. The platform used to develop and host web applications in data centers managed by Google. GAE is a cloud computing technology based on a set of computers and servers around the world and linked by a network. The App Engine applications are easy to build and maintain. They easily withstand the increased traffic load and the growing needs of data storage. Other cloud platforms include similar offers such as Amazon Web Services and Azure Services. Therefore, the proposed solution is hosted and deployed in GAE and does not represent a centralized solution because it is stored in grid computing scattered around the world. It is based on a client/server architecture based on the RPC (remote procedure call) of Google Web Toolkit (GWT). Figure 1 shows the different modules required to invoke a service. Each service has a small family of utility classes and interfaces. Some of these classes, such as the proxy service, are automatically generated in transparency via the user. The model of utility classes is the same for all implemented services. This allows us to quickly familiarize with the RPC.

A basic clustering model for faulty node detection could be modeled by assuming a set of clusters $S = \{s_1, s_2, s_3, s_4 \ldots . s_p$ with the compactness defined asC, the clustering schema could be obtained as

$$C_p = \frac{c}{\sum_{i=1}^{s} (\frac{\sum \mu_{ij}{}^2 ||x-v||}{\sum \mu_{ij}{}^2}} \qquad (1)$$

where μ denotes the membership function corresponding to the i cluster. The difference term in the denominator denotes the Euclidean distance function. Equation (1) denotes the degree of compactness of the given cluster. On the contrary, with the same assumptions as above, the degree of separation of cluster is given as

$$S_p = \frac{\sum_{i=1}^{s} \min ||v_i - v_c||^2}{c} \qquad (2)$$

IV.RESULTS AND DISCUSSION

The proposed algorithm has been implemented and tested with five sets of repository training data (Bache and Lichman, 2013). The first is the Iris dataset which contains three clusters. Each one refers to a type of plant from the Iris. The second is the Dermatology dataset which contains 34 attributes which 33 are assessed linear and one of them is nominal. It concerns a differential erythematous-squamous diseases diagnosis. The third is the Australian Credit Approval which concerns card applications credit. It contains 690 instances, each instance formed by 14 attributes. All attributes names and values have been changed to meaningless symbols to protect confidentiality of the data. The data is divided into two clusters. The fourth is the Breast Cancer Wisconsin dataset which contains two clusters of cancer breast. It concerns a breast cancer diagnosis reflecting the chronological data grouping. The last is the Mammographic Mass dataset which can be used to predict the severity (benign or malignant) of a mammographic mass lesion. It contains 960 instances.

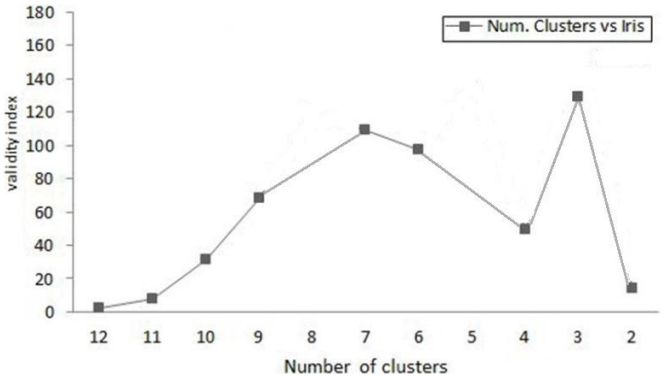

Figure 2. Cluster analysis plot

Since, it is essentially a detection based problem, the conventional efficiency parameters like True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are used to describe Precision, Recall and accuracy of the retrieval system.

$$precision = \frac{tp}{tp+fp} \qquad (2)$$

$$recall = \frac{tp}{tp+fn} \qquad (3)$$

$$accuracy = \frac{tp+tn}{tp+tn+fp+fn} \qquad (4)$$

On training and validating the feature set, the test input has

achieved an accuracy of approximately 95% with a 3 – 5 % marginal increase over fuzzy and SVM techniques.

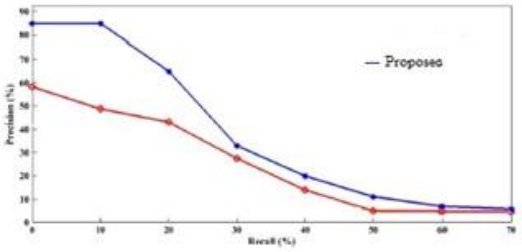

Figure 3. Recall rate accuracy for proposed method

The above figure illustrates a graphical plot of the obtained root mean square error against the patch size or window size. As the window size increases the error is found to converge. The convergence time is also drastically reduced which is a characteristic feature of compressive sensing and sparse representation. The reduction in error convergence reduces the computational time and thereby consequently reducing the computational complexity. Root mean square is a dimensionless quantity.

V.CONCLUSION

Ad hoc network security has come into the lime light of network security research over the past couple of years. However, little has been done in terms of defining the security requirements specific to MANET's. Such security requirements must include countermeasures against node misbehavior in general and denial of service attacks in particular. In this paper, we used the concepts of multi-stage dynamic non-cooperative game with incomplete information to model intrusion detection in a network that uses a host based IDS. We believe that this game-theoretic modeling is more realistic than previous modeling techniques. As part of our future work, we intend to extend our game theoretic approach to include selfish nodes.

REFERENCES

[1]Yongguang Zhang, Wenke Lee and Yi- An Huang, "Intrusion detection techniques for mobile wireless networks", Mobile networks and applications, pp. 1 – 16, 2003.

[2]Jin Hee Cho and Ing Ray Chen, "Model based evaluation of distributed intrusion detection protocols for mobile group communication systems", Wireless personal communications, Vol. 60, pp. 725 – 750, 2011.

[3] B. Wu, J. Wu, and Y. Dong, "An efficient group key management scheme for mobile ad hoc networks," International Journal of Security and Networks, Vol. 4, No. 1, 2009, pp. 125-134.

[4] Vydeki D and R.S. Bhuvasneswaran, "Effect of clustering in designing a fuzzy based intrusion detection for mobile adhoc networks", Journal of computer science, Vol. 9, No. 4, pp. 521 – 525, 2013.

[5]Priyanka Dahiya and Alka Chaudhary, "Fuzzy Based Intrusion Detection System in Mobile Ad Hoc Networks", International Journal of Computer Applications", pp. 45 – 47, 2014.

[6] Madjid Khalilian, Norwati Mustapha, Md Nasir Sulaiman, Ali Mamat, "Intrusion Detection System with Data Mining Approach: A Review", Global Journal of Computer Science and Technology, Volume 11 Issue 5 Version 1.0 April 2011

[7] S.S.Chopade and N.N.Mhala, "A Co-Operative Intrusion Detection System in Mobile Ad-Hoc Network", International Journal of Computer Applications, Vol. 18, No.6, pp.34-39, March 2011.

[8] Aikaterini Mitrokotsa1, Nikos Komninos2, and Christos Douligeris, " Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks", International Journal of Network Security, Vol.10, No.2, PP.93–106, Mar. 2010.

[9] Jerril Mathson Mathew and Lekshmy P Chandran, "Parallel implementation of fuzzy clustering algorithm based on map reduce computing model of Hadoop – A survey", International journal of computer science and information technologies, Vol. 6, No. 5, pp. 4740 – 4744, 2015.

[10] H. C. Huang, Y. Y. Chuang, and C. S. Chen, "Multiple kernel fuzzy clustering,"IEEE Trans. Fuzzy Syst., vol. 20, no. 1, pp. 120–134, Feb. 2012.

[11] Xianfeng Yang and Pengfei Liu, "A new algorithm of the data mining model in cloud computing based on web Fuzzy clustering analysis", Journal of theoretical and applied information technology, Vol. 49, No. 1, 2013.

[12] Pandeeswari and Ganesh Kumar, "Anomaly detection system in cloud environment using Fuzzy clustering based ANN", Mobile network applications, Vol. 21, No. 494, 2016.

[13] Bakshi A, Yogesh B, "Securing cloud from DDOS attacks using intrusion detection system in virtual machine", in

proceedings of second International Conference on Communication Software and Networks, pp. 260–264, 2010.

[14] Gang W, Jinxing H, Jian M, Lihua H, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Expert System Applications, Vol. 37, No. 9, pp.6225–6232, 2010.

[15] Oktay U, Sahingoz, "Attack types and intrusion detection systems in cloud computing", in proceedings of 6th International Information Security & Cryptology Conference, pp. 71–76, Turkey, 2013.