ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Critical Analysis of Anomaly Intrusion Detection Techniques in MANET

S.V.Shirbhate
Vinayak vidya mandir
Amravati, India
san_shirbhate@yahoo.co.in

Dr V.M.Thakare
S.G.B.A.U
Amravati, India
vilthakare@yahoo.co.in

Dr S.S.Sherekar
S.G.B.A.U
Amravati, India

ss_sherekar@rediffmail.com

Abstract- As mobile ad hoc network (MANET) has become very important technology, research concerning its security problem, especially, in intrusion detection has attracted many researchers. Various approaches have been proposed for intrusion detection in mobile network. However, little research work has been done in actually implementing them, especially for anomaly detection in mobile networks. Due to vulnerabilities introduced by mobility, anomaly based detection techniques are more crucial in MANET than misuse based detection technique. This paper focuses on various anomaly detection techniques for MANET and perform critical analysis in various methods of anomaly intrusion detection.

Keywords: Anomaly Intrusion detection, Mobile ad hoc network, security.

I. INTRODUCTION

In the recent years, wireless technology has tremendous rise in popularity and usage. It is one of the opening fields in the domain of networking. Mobile ad hoc network (MANET) is a collection of mobile hosts without the required interference of any existing infrastructure or centralized access point such as a base station. Due to the inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks [1]. Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective. Hence there is need of intrusion detection systems that monitors the network and detects the misbehavior or anomalies and also notifies other nodes in the network to avoid the misbehaving nodes [2].

The ultimate goal of security solutions for wireless network is to provide security solutions such as integrity, confidentiality, availability, security authentication and non-repudiation to a mobile users. The major task of intrusion detection system is to discover the intruders from network packet traffic data or system audit data. In this paper the intrusion detection technique for MANET are introduced. Specifically the anomaly detection techniques in MANET are analyzed.

The remainder of the paper organized as follows, section II elaborates the methodology for intrusion detection system, section III describes the evaluation performance of anomaly detection methods section IV contains the tabular information of anomaly detection methods, in section V analyzed and discuss on these methods and at the section VI finally conclude by discussing the outcome of study.

II. METHODLOGY FOR INTRUSION DETECTION SYSTEM

As the computers have been networked together, the security in computer network becomes a critical issue. The evolution of the internet has increased the need for security system and this has led to the search for the best ways possible to protect our systems. Intrusion detection system is used to monitor network traffic and detect if the system is targeted by network attack [3]. Intrusion detection is used in the networks by comparing the set of baselines of the system with the present behavior system. Thus the basic assumption is that the normal and abnormal behavior of the system can be characterized.

Intrusion detection is an important part of computer security in wireless network. It provides an additional layer of defense against computer is use after physical, authentication and access control [4].

Basically in intrusion detection system, Misuse or signature and anomaly detection techniques are used. Misuse detection relies on the use of specifically known patterns of unauthorized behavior. Anomaly detection describes the abnormal pattern by measuring deviation from a normal behavior or profile. The assumption of this type of detection is that attacks are events distinguishable from normal legitimate use of system resources [5]

As the vulnerabilities introduced by mobility, anomaly based detection techniques are more crucial in mobile network than misuse based detection techniques. However designing them is challenging because normal profiles are usually very hard to build and maintain due to mobility of nodes. The main limitation of anomaly based detection technique is that it generates higher false positive rate than misuse based detection technique because the entire scope of system behavior may not be covered during learning phase and legitimate behavior may change over time [6]. Hence establishing and maintaining normal profiles for nodes and improving the detection performance is crucial in designing an efficient anomaly detection technique in mobile network [7].

There are various methods for anomaly intrusion detection techniques. Some of them are discussed in next section.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

III. PERFORMANCE EVALUATION

In Mobility pattern based anomaly detection algorithm [7], each node's normal mobility profile is modeled as multi leaf structure. In this method the clusters are generated through data mining techniques and pattern strings are generated through fuzzy logic techniques which are fundamental elements of multi leaf tree structure. This algorithm is developed to detect potential internal attacker such as masquerades. This algorithm can achieve desirable performance in terms of false alarm rate(<=8%) and detection rate(>=90%) for the nodes with regular movement behavior. For a given design parameter $C_{thr,}$ the process of determining P_{thr} is adjusted by trial and error. If $C_{thr=}5.0$ and $P_{thr\ =}$ 0.6 then MPB algorithm achieves good performance in detection rate and false alarm rate for all the ranges of velocity.

In anomaly detection scheme using Dynamic learning method [1], the average of difference for each time slot is calculated as the feature.

The average difference between the Dst_Seq in RREQ message and one held in list are calculated as follows.

When sending or forwarding a RREQ message, each node records the destination IP address and Dst_Seq in its list. When RREP message is received, the node looks over the list to see if there is the same destination IP address. If it does exist, the difference of Dst_Seq is calculated. This operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as feature. In this method, the traffic that flow across each node is expressed in time slot i by three dimension vector $\mathbf{a_i=(a_{i1},a_{i2},a_{i3})}$. Here the groups of normal states are considered to be gathered close in feature space and abnormal state to be considered to be the scattering data deviates from cluster of normal state.

The mean vector $\bar{a}^{\mathbf{D}}$, using training data set D of N time slots is calculated as follows

$$\bar{a}^{\mathbf{D}} = \frac{1}{N}\sum_{i=1}^{N} a_i$$

Then calculate the distance from input sample a to mean vector $\bar{a}^{\mathbf{D}}$ as

$$d(a)=\|a- \bar{a}^{\mathbf{D}}\|^2$$

If distance larger than threshold T_h, then it will judged as attack

$d(a)> T_h$: attack

$d(a)<= T_h$: normal

Where T_h= the projection distance with maximum value from learning data set

$T_{h=} d(a_I)$, where $I = \arg \max d(a_i)$

Let $\Delta T0$ be the first time interval for a node participating in MANET. By using data collected in this time interval, the initial mean vector is calculated, then the calculated mean vector will be used to detect the attack in the next period time interval ΔT .If the state in ΔT is judged as normal, then the corresponding data set will be used as learning data set. Otherwise, it will be treated as data including attack and it will be consequently discarded. In this way, the normal state of network is learning.

In profile based intrusion detection system [8], each node monitors its neighbor traffic and builds a profile for each of its neighbors. The profile includes all features such as packet type, flow direction, statistics measures. This measures use as threshold to detect intrusion. Mean and standard deviation are calculated for each sample of data. The set of upper and lower values for anomaly has to be prepared. Once the traffic feature exceeds the threshold, an alert should be produced. The node can use the profile to monitor the neighboring node's behavior. In this method a statistical modeling approach is used to analyze the behavior. For any random traffic packet of value x gathered from n observation of user A, the statistical model determines whether the next new traffic packet x_n +1 observed from the user B is abnormal with respect to the previous observations. A new observation x_n +1 is abnormal if it falls outside a behavioral interval defined.

In agent based anomaly intrusion detection system [4], home agent gathers information from its own system and mobile agents gathers information from neighboring system to identify any attack. In this method, each feature or character vector f in training data set is divided into C_i classes using Bayesian classification. Then average probability for each feature vector is calculated and saves in probability distribution matrix M. A decision threshold is learned from the training data set. Normal profile is created using threshold value. If the probability is greater than threshold value it is labeled as normal, otherwise it is labeled as abnormal.

In K-means clustering method [9], k-means algorithm is used to construct the centroids of clusters. Features of nodes are events such as sending, receiving, drop and forward packets are given as input to algorithm. These features are selected from trace file. In this method two clusters are created one for normal and another for abnormal or intrusive behavior. Proposed IDS is host based which monitor each and every node in the network whether any node in network generates events or not.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

IV. TABULAR INFORMATION

Table 1 Performance Analysis Of Various Anomaly Intrusion Detection Techniques Used In Manet For Ids

S. NO	Methodology	Author	Yr. of publication	Approach	Parameter used	techniques	compensation	confines
1.	Mobility pattern based method	Chaoli et al.	2008	Multi – leaf structure	Distance measurement C_{thr} & P_{thr} are design parameters for creating clusters & pattern strings resp.	Data mining & fuzzy logic	1. Easily generating & maintaining the normal profile. 2. Solving more challenging problem of handling many closer pts &mobility pattern. 3. Achieving fairly good performance without string. assumption 4. Determining the design parameter, threshold efficiently.	It is not suitable for nodes with totally random movement behavior
2	Anomaly detection scheme using Dynamic learning method	Santoshi et al.	2007	dynamic training method updated at regular time interval	1.ΔT_0 be the first time interval for node participating in MANET 2. Initial mean vector i.e. $\bar{a}^D = 1/N(\sum a_i)$is calculated. 2. ΔT is next time interval	Data mining (clustering)	1. Dynamically updated training data method shows significant effectiveness in detecting black hole attack.	For shorter updating interval, the more processing overhead is needed. Hence e more battery power will be consumed.
3.	Profile based neighbor monitoring mechanism	R.Samina than et al.	2010	Indexed Profile based mining and statistical modeling approach	1. Traffic pattern (M) are mined from traffic data set 2. Pattern summarization to find k pattern profile based on pattern set M	clustering	1. PROFIDES work in highly dynamic varying environment 2. It controls the traffic intensity 3. It detects the intrusions earlier in time as well as updated to user profile.	In this method intrusion attempts can be characterized by sequence of user activities that leads to uncompromised system states.
4.	Agent based method	Nakkeera n et al.	2010	Agents &data mining (Bayesian classification)	1. Character vector or feature F, classifier C is learned from training data set using naïve Bayesian classification algorithm , probability P.	Local integration , global integration, Data mining (naïve Bayesian)	1. This system not only blocks the application oriented issues but it stops some of the network security issues. 2. This system act as an intrusion prevention system.	Intrusion prevention system can generate more false alarms.
5.	Overhearing packet transmission of neighboring nodes	S.Madhav i et al.	2008	Monitoring the nodes & statically calculate the threshold	P%=L is total link capacity T= Time period r% is link capacity used by neighboring node. S% is link capacity being wasted due to collisions, garbage data & flows that did not reserve bandwidth.	Applying simple rule to identify the intruder information	Not only detecting attacks but also responding to attacks	Since mobile ad hoc nodes typically have limited battery power, it is not efficient to make each node always a monitoring node and especially when threat level is low.
6.	Clustering unsupervised learning process	P.K.Karm ore et al.	2011	Two clusters are created. One for normal & another for abnormal Calculate the mean square error of feature data & check Euclidean distance from	Throughput, packet delay, packet loss	K- means clustering method of data mining	It improves the detection rate and decreases the false alarm rate.	In this technique throughput increases as no. of normal increases.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

				centroid				
7.	Architecture model EADAN (Enhanced Intrusion Detection Techniques for MANET)	L.Prem Rajeswari et al.	2007	Various logical components are designed for specific purpose	Sequence number, time, IP address of the node, hop count, packet size.	AODV routing protocol	1. System does not utilized any cryptographic mechanism to ensure protection from malicious activities 2. It does not introduce any additional computation overhead to the routing process 3. It does not require thev sending of additional packets. Thus it does not consume the available bandwidth.	

If any, the feature of that node is extracted and calculates the mean square error and then check Euclidean distance from centroid. If it is nearest to normal cluster centroid then IDS will assume that the node is normal and it will allow to process event normally. If it is nearest to abnormal clusters, it will not allow processing i.e. IDS will drop that event from queue which is generated by malicious node. Data mining method is used in this method to improve the efficiency and effectiveness of MANET nodes.

Enhancement on intrusion detection system for MANET [6] based on a novel architecture that uses intrusion detection techniques to detect active attacks that can perform adversary against routing fabric of mobile ad hoc networks. Its logical components are traffic interception module, event generation module, attack analysis, counter measure module. Traffic interception module captures the incoming traffic from network and selects which of these packets should be further processed. Event generation module is responsible for abstracting the essential information required for attack analysis such as sequence number, time, IP address of the node, hop count, packet size. The attack analysis module verifies type of attack. Countermeasure module is responsible for taking action against attacks. This method analyses whether received packet is normal or malicious routing packet.

V. ANALYSIS AND DISCUSSION

In Mobility pattern based anomaly detection algorithm, a given clusters threshold (C_{thr}), determining the value of pattern string (P_{thr}) is adjusted by trial and error. Hence selecting the value of P_{thr} must be ideal value for good performance in terms of false alarm rate and detection rate.

In anomaly detection scheme using Dynamic learning method if mobility rate become faster, detection accuracy of the proposed method ($\Delta T = 300(s)$) and ($\Delta T = 600(s)$) than the using initial training data only. However, the detection accuracy of the proposed method degrades when the updating time interval become longer. Hence proposed scheme is effective in anomaly detection.

The profile based intrusion detection system evaluates the performance in terms of traffic intensity, mobility rate, packet drop, number of attacks occurred.

The traffic intensity = (no. of packets received / no. of packets sent) *100

Mobility factor = Rate at which the nodes are moving from source to destination.

In this method each node can monitor its neighbor's behavior, the system can detect whether a node has forwarded a routing packet or not. It is observed that packet drop increases when the node mobility rate increases. The intrusion detection process carried out PROFIDES was beneficial because it detects earlier in time as well as updates to user profile which isolated such nodes from normal activity. As compared to AODV protocol PROFIDES detection rate is better while detection is faster. The performance was evaluated based on metrics such as attack identification rate, packet drop rate, traffic intensity between nodes and mobility ratio which will improve the effectiveness and reliability with security in MANET.

In agent based anomaly intrusion detection system anomaly, local integration and global integration detection modules are considered. The performance of these detection modules are in terms of detection rate and false positive. In this proposed system detection rate is high and it encourages the system. The detection rate for anomaly detection (A), local Integration (D), global integration (E) are 80%, 95.41%, 94.33% respectively and false positive rate are 1%. 0.8%, 0.75%. From this observation, proposed system shows that detection rate is increased and false positive rate is decreased as compare to other mechanism.

The intrusion detection method using k-means clustering is improved throughput, packet delay and packet loss. By improving this network parameter, the performance of network is enhanced.

VI. CONCLUSION

In this paper, critically reviewed some existing anomaly based intrusion detection system. It is found that some of these existing systems are faced with drawbacks. The main limitation of an anomaly based detection technique is that it generates higher false positive rate than misuse based detection technique. It is also found that the entire scope of system behavior may not be covered during learning phase and legitimate behavior may change over time. In anomaly detection technique, establishing and maintaining normal profiles for nodes and improving the detection performance are critical in designing an efficient anomaly detection algorithm in mobile network. Hence there is need to develop

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html

a new architecture and mechanism to protect the wireless networks and mobile computing applications.

VII. REFERENCES

[1] Santoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile AdHoc Networks By Dynamic Learning Method", International Journal Of Network Security ,Vol.5, No.3, pp.338-346,Nov,2007.

[2] S.Madhavi, "An Intrusion Detection System In Mobile Ad Hoc Networks", International Conference On Information Security And Assurance published in IEEE Computer Society,978-0-7695-3126-7/08,pp.7-14,2008.

[3] C.Xiang, M.Y.Chong and H.L.Zhu, "Design Of Multiple-Level Tree Classifiers For Intrusion Detection System", proceedings of IEEE conference on Cybernetics and Intelligent Systems Singapore,0-7803-8643-4-04, pp. 873-878,2004.

[4] R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc Networks", International Journal of Engineering and Technology (IACSIT) Vol. 2, No.1, February, 2010.

[5] S. Kannan, T. Kalaikumaran, S. Karthik and V. P. Arunachalam, "A Study on Various Attack Detection Methods in Mobile Ad-Hoc Networks", International Journal of Signal System Control and Engineering Application 3(3)ISSN: 1997-5422 published in Medwell Journals,pp.34-39,2010.

[6] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, "Enhanced Intrusion Detection Techniques for Mobile Ad Hoc Networks", IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES), pp.1008-1013, Dec 20-22, 2007.

[7] Chaoli Cai and Ajay Gupta , "Mobility–Pattern Based Anomaly Detection Algorithm in Mobile Networks", This full paper was peer reviewed at the direction of IEEE communication Society subject matter expert for publication in the ICC2008 proceedings.978-1-4244-2075-9/08, pp.1680-1684,2008.

[8] R. Saminathan, Dr. K. Selvakumar, "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network", International Journal of Computer Applications 0975 – 8887 Volume 7– No.14, October 2010.

[9] Preetee K. Karmore , Smita M. Nirkhi, "Detecting Intrusion on AODV based Mobile Ad Hoc Networks by k-means Clustering method of Data Mining" International Jo urnal of Computer Science and Information Technologies, (IJCSIT) Vol. 2 (4) pp.1774-1779, 2011.

CONFERENCE PAPER
National Conference on Information and Communication Technology for Development
Organized by PRMITR, Amravati (MS) India
http://mitra.ac.in/forthcoming.html