Efficient Detection of Intrusion Using Inner and Outer Boundary Models with Transductive Learning Concept in Mobile Adhoc Network

R.M.Chamundeeswari1, Dr P Sumathi2
1Assistant Professor, Department Of Computer Application, Asan Memorial College Of Arts & Science, Chennai , rmp.chamu79@gmail.com
2Assistant Professor, PG and Research Departement of Computer Science ,Govt Arts College ,Coimbatore
sumathirajes@hotmail.com

ABSTRACT: Intrusion detection system (IDS) plays a very significant role for sensing different types of attacks in Mobile Ad-hoc Network (MANET). The main function of intrusion detection includes both monitoring and analyzing both the user and activities of the mobile network. Research works conducted on Dynamic Anomaly Detection (DAD) confirmed the uniqueness and topology of the network but was not feasible on analyzing intelligent detection schemes. Quantify Network Dynamism (QND) influenced the mobility from different perspectives but failed in effective designing of concrete data diffusion. QND plan still need to address the qualitative performance metrics on the mobility models. To obtain a feasible solution in analyzing the anomalies in MANET, Orthomorphic Analyst k-Nearest Neighbor (OANN) method and Report based Outlier Detection (ROD) mechanism is developed with i-boundary values in this paper. Orthomorphic Analyst k-Nearest Neighbor uses the mathematical mapping to analyze the correct angles of anomalies within the specified node range in MANET. OANN analyzes i-inner boundary values of the anomalies, and performs the intelligent detection in MANET. Diffused (i.e.,) spread intrusions on the outer i-boundary values are detected using the ROD mechanism. Reporting in ROD mechanism records the repetitive probabilistic dropping of data packets with outer 'i' boundary values in MANET. Finally, Transductive learning concept merges the OANN method and ROD mechanism into one single step to address the measures of reliability for the entire boundary values in MANET. With the analyzed angle by OANN and ROD applies transductive concept to calculate a score value and helps to identify whether an intrusion is detected or not. OANN and ROD with Transductive learning concept conduct experiments on the performance factors such as outlier detection accuracy in MANET, true positive value of transductive concept, the inner boundary analyzing efficiency, runtime for analyzing the outer boundary intrusions.

Keywords: Orthomorphic Analyst k-Nearest Neighbor, Mobile Ad-hoc Network, Report based Outlier Detection, Intrusion Detection, Transductive Learning Concept, Anomalies.

1. Introduction

A mobile Ad-hoc Network (MANET) is comparatively novel communication model which does not have expensive base stations or wired infrastructure. Every mobile node in MANET is equipped with a wireless transmitter and receiver communicates with other mobile nodes within the radio communication range. Social network analysis performed in [3] were dependent on social investigation of a node's past interactions and consisted of three locally evaluated components but were not effective enough in measuring the accuracy.

MANET has turned out to be an exciting and significant technology in recent years since the inception and propagation of the wireless devices. MANET is tremendously vulnerable to attacks due to the open medium, arbitrarily changing network topology and lack of centralized monitoring point. The different types of attacks related to MANET are flooding, black hole, warm hole, packet dropping and Byzantine attack. At this juncture, there arises a need to identify new methods and mechanisms to ensure safe communications between the nodes in the wireless networks and mobile computing application. Intrusion detection system (IDS) tools are appropriate for recognizing these attacks. IDS examine the network activities by means of audit data and use patterns of well-known attacks to sense potential attacks.

Cognitive radio network based on IEEE wireless regional area network illustrated some of the potential attacks

against it. The CRN rapidly sense a simple yet effective IDS was then presented in [17]. The IDS adopted an anomaly detection scheme that kept the CRN system limit through a knowledge phase. So, it was highly capable to detect novel types of attacks.

The dependency and decentralization natures of MANET allows a malicious nodes to extent new type of attacks that in a way has a higher influential factor on the part of cooperative algorithms. Moreover due to their open medium, MANET is highly vulnerable to different types of attacks like passive eavesdropping, dynamic impersonation, and denial of services. Home agents present in each system as demonstrated in [6] collected the data from its own scheme and using data mining techniques watched the local anomalies. In order to avoid the anomaly intrusion in MANETs, mobile agents and data mining techniques played a major role.

Anonymous Location-based Efficient Routing proTocol (ALERT) as expressed in [7] first divided the entire network into zones and in turn selected the intermediary relay nodes which were present in the zones for effective communication. In addition, it hides the data received in the middle of many initiators to make stronger source and destination anonymity protection but failed to attempt to thwart stronger, active attackers and demonstrated comprehensive results.

Multicast Authentication Based on Batch Signature (MABS-B) avoided the correlation between packets in [19] and provided measures for perfect resilience to loss of packets. As a result, MABS-B was efficient in terms of latency, computation, and communication overhead due to a resourceful cryptographic primitive called batch signature, which supported the authentication of any amount of packets simultaneously.

Intrusion detection system (IDS) tools are suitable for identifying the attacks. In genetic algorithm, Bayesian network is constructed over the collected features and fitness function was calculated in [13]. Based on the fitness value the features were selected. Markov blanket discovery also used Bayesian network and the features were selected depending on the smallest amount description length but failed to combine the entire features to produce a desired result for different type of attacks. On the other hand, the framework was provided for intrusion detection system and was effectively classified in [20] that largely identified the misbehaving activities and also provided protection.

An intruder that cooperate a mobile node in MANET destroys the communication between the nodes by broadcasting fake routing information, providing incorrect link state information or overflowing other nodes with redundant routing traffic information. Therefore, successful implementation of MANET depends on user's self-assurance in its security. The security research in MANET has paying concentration on key management, routing protocol and intrusion detection techniques. Anti-Detection moving strategy for mobile sink as presented in [4] selected a trajectory for mobile sink node. The sink node minimized the total number of message communication between all the static sensor nodes to the mobile sink node but failed to provide the opportunity for being sensed by the adversaries.

Intrusion detection is used as a successive line of protection in Mobile Ad-hoc Networks. The protection was carried out in [18] using five supervised categorization algorithms for intrusion exposures. The protection mechanism measured their performance on a dataset, which consisted of dissimilar traffic conditions and mobility model for multiple attacks. However, the goal was to categorize the report based on the difficulty cost matrix in MANET.

Enhanced Adaptive Acknowledgment (EAACK) was particularly intended to handle malicious behavior rates in [6]. As represented and executed a fresh intrusion detection method, EAACK did not really influence on the network performances. EAACK was not possible of adopting hybrid cryptography techniques to reduce the network overhead origin by digital signature. The data fusion model that was based on the

Dempster–Shafer as designed in [10, 11] was designed in such a way that whether user authentication was required or not and also was based on the biosensors that can be selected as a security measure. The decisions were made in a fully distributed manner by using the authentication device and IIDS but at the cost of the computation complexity. The continued user-to-device authentication as a result is considered to be the demanding task in high security MANET.

The nodes in Intrusion Detection System (IDS) are designed in mobile ad hoc network to identify and prevent black hole attacks. The IDS nodes were set in sniff mode in order to perform Anti-Blackhole Mechanism (ABM) function in [14], which is mostly used to estimate an apprehensive value of a node according to the abnormal difference between the routing messages transmitted from the node. An intrusion detection system developed for detection and separation of attacks in [16] and Mac layer applications were used for detecting malicious activities and focus was made on the identification of attack sequences in the network.

An anomaly detection scheme that was designed on the basis of dynamic learning process was illustrated in [1] allowed the training data to be changed at different time intervals. The dynamic learning process designed for anomaly detection involved the projection distances calculated using the multidimensional statistics and a forgetting curve. Dynamic Anomaly Detection (DAD) Scheme usually used to confirm the uniqueness and the topology of the network but the study was not feasible on analyzing the more intelligent detection schemes.

In this work, Orthomorphic Analyst k-Nearest Neighbor (OANN) method and Report based Outlier Detection (ROD) mechanism with i-boundary values is used for the effective detection of intrusions in MANET. OANN uses the intrusion to be detected on the inner boundary and performs the intelligent detection in MANET. ROD mechanism is used on the outside outer boundary intrusion detection by probabilistic analyzing the dropping of packets. Then Transductive learning concept merges the OANN method and ROD mechanism with score value. The score value into one single step address effective communication by removing all the intrusions.

The structure of paper is as follows. In Section 1, the various types of intrusion detection in MANET is explained with limitations. In Section 2, the Orthomorphic Analyst k-Nearest Neighbor, Report based Outlier Detection and Transductive learning concept is demonstrated. Section 3 describes the simulation environment with parametric factor description. Section 4 explains the result values on the inner and outer boundary of MANET. Section 5 illustrates the related work and finally concluded the work in Section 6.

2. System Architecture Of Combining Inner And Outer Boundary Intrusion Detection In Manet

Inner and Outer Boundary intrusion Detection identifies intrusive activities in MANET and combines the system using transductive learning concept. The inner intrusion detection uses the Orthomorphic Analyst k-Nearest Neighbor (OANN) method with 'i' boundary values for the detection. The outer boundary detection uses the Report based Outlier Detection (ROD) mechanism with 'i' boundary values. The inner and outer boundary combined with transductive learning concept in MANET removes all the intrusions on varying performance parameters. The overall architecture diagram of inner and outer boundary of intrusion detection in MANET is illustrated in Fig 1.

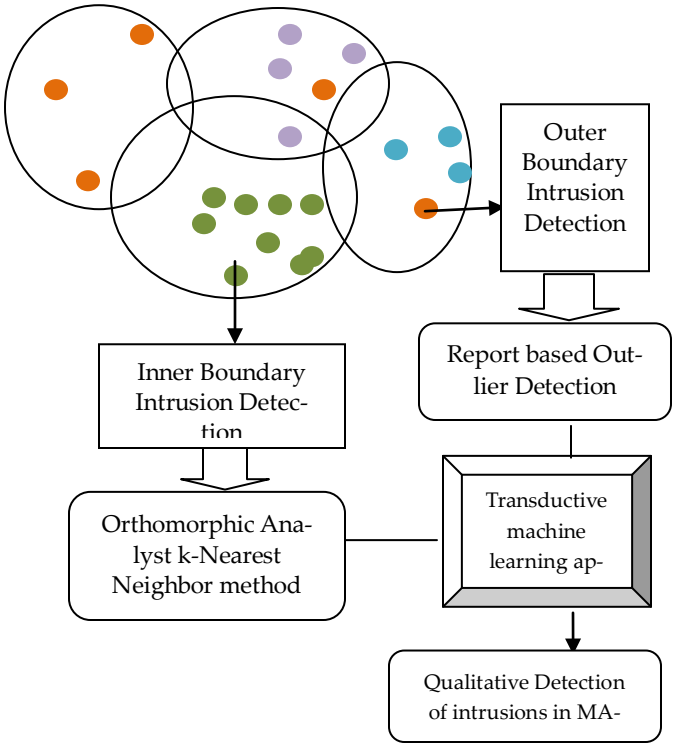


Fig 1 Overall Architecture Diagram of Inner and Outer Boundary Intrusion Detection in MANET

Mobile Ad-hoc Network holds different boundary of nodes with movable pattern. The nodes move from one place to another but within the specified distance. Sometimes, the movement of nodes within the boundary causes the traffic in MANET which leads to intrusions. Orthomorphic Analyst k-Nearest Neighbor method detects the intrusion activity based on the traffic intensity at inner boundary instance within the communication mobile ad-hoc system. Orthomorphic analyze the nearest neighboring nodes position using the mathematical mapping of angles with 'i' inner boundary values in mobile network.At the time of the mobile node movement inside the specified distance, sometimes the nodes also reach the outlier region in MANET. The outlier region nodes create malicious attacks on that specified boundary which leads to the dropping of packets. To overcome the outlier detection in mobile network, Report based Outlier Detection (ROD) mechanism is introduced for outside 'i' boundary value. ROD mechanism reports the dropping of packets (i.e.,) detecting of intrusions in the MANET.

OANN method and ROD mechanism is combined together with the Transductive learning concept in MANET. Transductive learning concept in mobile network is developed to merge OANN and ROD and finds rules to compute an original intrusion detected score value. The major benefit of the transductive learning concept in MANET is that the decision function is generated only to the particular intruded node for detection. It reduces the runtime, as the generation of decision function is not performed on the entire boundary space. The decision functions in mobile network identify intrusion nodes differently with qualitative result. The elaborate work of OANN and ROD mechanism is discussed briefly in the forthcoming sections.

2.1 Orthomorphic Analyst k-Nearest Neighbor Method

Orthomorphic Analyst k-Nearest Neighbor (OANN) method evaluates the mathematical mapping to determine the correct angles of anomalies within the 'i' boundary values in MANET. The OANN method performs the mathematical mapping using the Orthomorphic (i.e.,) Angle based Distance measurement between the node points for easy detection of traffic creating nodes. The Orthomorphic distance measure each distance between the pair of mobile nodes and evaluate the correct angle of position within the 'i' inner boundary. The mobile node with the previously defined position and newly computed position using the OANN method is used to easily analyze the intrusion nodes in MANET. Traffic Intruded MANET and the intrusion analyzed with OANN method processing is shown in Fig 2 (a) and (b),

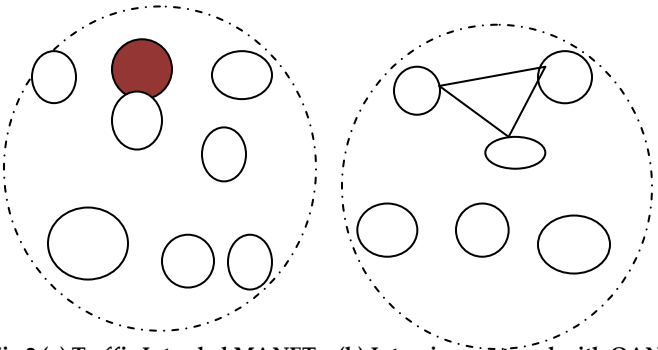
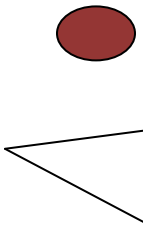


Fig 2 (a) Traffic Intruded MANET (b) Intrusion analyzed with OANN



- Intruded Nodes in inner boundary MANET

- Angle used for intrusion analyzing

Fig 2 (a) demonstrates the traffic intruded mobile ad-hoc system. The intruded node is identified in Fig 2 (b) using the OANN Method. The mathematical mapping with correct angle is used to easily identify the traffic intruded nodes in the mobile ad-hoc network. Let us assume that 'i', 'j' as the pair of mobile nodes with boundary points 'b'. OD_i^p is defined as the sorted sequence of the mobile nodes within the boundary points. The inner boundary nodes between 'i and 'j' nodes in the sequence is denoted as $N_{i,j}^b$.

$$Inner\ Boundary\ Nodes = N_{i,j,\ldots n}^b \quad \ldots\ldots\ldots\ldots \text{Eqn (1)}$$

Similarly, Eqn (1) describes the 'i,j,….n' as the pair of mobile nodes in the predefined position for 'i' inner boundary values. The measure of the Orthomorphic distance is the ratio of summing up of all the 'k' nearest neighboring nodes distance, to effectively analyze the traffic intruded nodes in mobile network. Orthomorphic Distance (OD) between sources to destination node in mobile ad-hoc network is defined as,

$$Orthomorphic\ Distance = \sum_{i=1}^{k} N_{i,j,\ldots n}^b \quad \ldots\ldots\ldots\ldots \text{Eqn (2)}$$

Eqn (2) describes the correct angle of traffic intruded using the Orthomorphic Analyst k-Nearest Neighbor (OANN) method with 'n' mobile nodes for 'i' inner boundary values.

2.2 Report based Outlier Detection (ROD) mechanism

The main objective of the report based outlier detection mechanism is to identify the top 'k' outliers of nodes in MANET which results in certain abnormal behaviors such as the dropping of packets. Report in ROD mechanism refers to the repetitive probabilistic dropping of data packets with outer 'i' boundary values in MANET. The development of report method in the outlier detection, leads to the improved communication system by removing the intrusion on the outer 'i' boundary of the MANET.

The report system in MANET clearly denotes the intruded mobile nodes and also identifies the packet dropping nodes in the outer boundary system.

$$Outer\ Boundary\ (OB) = 1 - \sum_{i=1} I_i * N_i \quad \ldots\ldots\ldots\ldots$$

Eqn (3)

The outer boundary (OB) denotes the product of the intruded mobile nodes and the number of mobile node count within the boundary, I_i Denote the intruded mobile nodes and N_i is the number of mobile node count within the boundary.

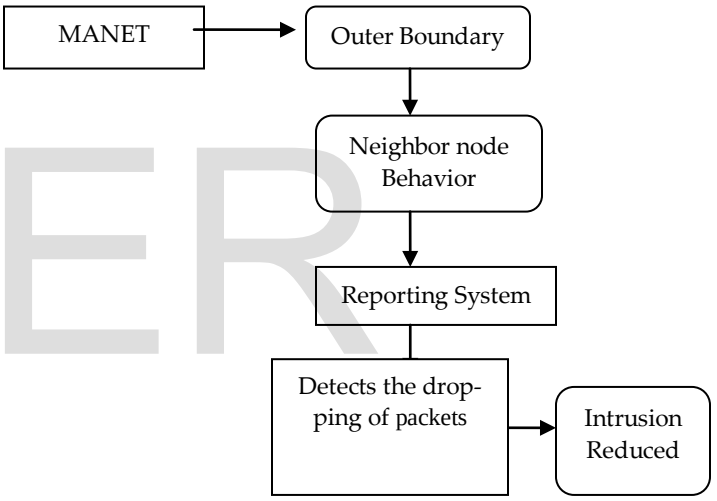


Fig 3 Framework of Report based Outlier Detection

The framework of Report based Outlier Detection with the outer boundary values in mobile network is demonstrated in Fig 3. The outer boundary contains the set of mobile nodes of particular range and also the intruded nodes from the different boundary range. The behavior of the neighbor node analyzes the outlier within the boundary and implements the report system. In MANET, the packet dropping is computed as,

$$Packet\ Drop\ in\ OB = Total\ No.of\ incoming\ packets\ to\ OB - Number\ of\ data\ packet\ dropped$$

…….. Eqn (4)

The packer drop in Outer Boundary (OB) is defined in Eqn (4) as the difference between the number of packet dropped and the total number of incoming packets within the outer boundary. ROD is used to easily analyze the drop of packets from the MANET with the help of Eqn (5)

$$ROD = N_i - I_i * Packet\ Drop\ in\ OB \quad \text{……..}$$

Eqn (5)

The intruded node is the one which drop the packets in MANET, and it is identified in ROD using the difference operator. The total no. of mobile node count within the outer boundary N_i in Eqn (5) easily detects the outliers in ROD framework.

In MANET, a system entity is denoted as the mobile nodes which are capable of observing the behavior of other entities and according to the behavior, the report operation is performed. A mobile node observes and records the abnormal behavior of neighbor's mobile nodes which are out of the specified range. As a result the report based outlier demonstrates the total amount of repetitive incoming packets that are observed for each neighbor.

2.3 Transductive learning concept

Transductive learning is used to merge the Orthomorphic Analyst k-Nearest Neighbor (OANN) method and Report based Outlier Detection (ROD) mechanism for effective detecting of intrusion and to calculate the score value. Transductive learning defines the inner and outer structure with the N_i in the MANET.

$$Transductive\ score\ value = N_i \sum_{i=1}^{k} (OD_{i,j,\ldots,n}^{inner\ boundary}); N_i (ROD_{i,j,\ldots,n}^{outer\ boundary} - OB) \ldots \text{Eqn (5)}$$

Transductive learning concept depend on the information obtained from the OANN and ROD (i.e.,) data dependent class for detecting the intrusions with the original score value. With this transductive score value, it helps to identify whether an intrusion is detected or not. If the score value is higher then there is a high rate of possibility for that mobile node to be an intruder node. Algorithmic step of Transductive learning concept in MANET with OANN method and ROD mechanism is described as,

Input: Set of mobile nodes with inner and outer boundary class

Output: Intrusion detected on the 'i' boundary values

// OANN method

Step 1: For i=1 to n, do compute the Orthomorphic Distance

Step 2: Performs Orthomorphic Distance on 'k' nearest neighbor within the inner boundary values

Step 3: End For

// ROD mechanism

Step 4: Neighbor Node Behavior analyzed on outer boundary system

Step 5: Packet dropping is computed using Eqn (4)

Step 6: Report based outlier demonstrates total amount of repetitive incoming packets observed for each neighbor

// Transductive learning concept

Step 7: Score value computed on inner and outer boundary in MANET

Step 8: Merges OANN and ROD for effective detection of intrusions

In Transductive learning concept, intrusion are detected in MANET and effective communication (i.e.,) data packet transfer is performed. Transductive learning concept employs the inner and outer boundary intrusion detection method using the computation of the original score value. With the help of this original score value, the anomalies in MANET are identified effectively. The inner boundary traffic intruded is avoided using the OANN method and outer boundary packet dropping is removed using the ROD mechanism.

4 Simulation Environment

Combining Inner and Outer Boundary Intrusion De-

tection with Transductive Learning concepts in Mobile Ad-hoc Network uses the ns-2 network simulator. The ns2 simulator uses the random surrounding data path of 1200 ×1200 size. The inner and outer boundary nodes in MANET hold 30 simulation milliseconds. The mobile networks continue for an effective detection of the intrusions with qualitative performance. Destination Sequence Based Distance Vector (DSDV) routing is performed in MANET with predefined information.

In the Random Way Point (RWM) model, each mobile node shift to an erratically chosen location. The RWM uses standard number of mobile nodes for data aggregation. The chosen location with a randomly selected speed contains a predefined amount and speed count. Combining Inner and Outer Boundary Intrusion Detection with Transductive Learning concept contains approximately of about 100 neighboring mobile nodes. The randomly selected position with a randomly selected velocity provides a predefined speed.

The minimum moving speed of OANN method and ROD mechanism is about 5.0 m/s of each mobile node. The experiment is conducted on the factors such as outlier detection accuracy in MANET, true positive value of transductive concept, the inner boundary analyzing efficiency, runtime for analyzing the outer boundary intrusions, and packet drop rate.

Outlier Detection is an observation that appears to deviate from other observations of nodes in MANET. Identifying an observation (i.e.,) outliers on the outer boundary of the mobile network as an outlier depends on the underlying distribution of the data packets among the nodes. True positive value (i.e.,) prediction is the event that the test makes a positive prediction on the mobile nodes while packet transfer. The subject has a positive result on the transductive concept.

$$Precison = \frac{\sum True positive\ score\ value}{\sum True\ Outcome\ Positive\ score\ value} \quad \text{..... Eqn (6)}$$

Eqn (6) describes the precision score value of transductive concept based on the node movement in the MANET. The inner boundary values of the MANET is analyzed efficiently by removing the traffic intruded nodes with Orthomorphic distance. Runtime is defined as the amount of time taken for analyzing the outer boundary intrusions and to remove the intruded nodes. The intruded node leads to packet loss, and packet loss is defined as the amount of data packets dropped in the mobile ad-hoc network. The packet drop is expressed in MANET as,

$$Packet\ Drop\ in\ OB = Total\ no.of\ incoming\ packets\ in\ OB - Number\ of\ data\ packet\ transmitted\ percentage \text{..... Eqn (7)}$$

The packet dropping is defined as the difference between the total numbers of incoming packets and the number of packet transferred.

5. Result Analysis On Inner and Outer Boundary

Combining Inner and Outer Boundary Intrusion Detection (IOBIDS) with Transductive Learning concepts in Mobile Ad-hoc Network is compared against the existing Dynamic Anomaly Detection (DAD) Scheme and Quantify Network Dynamism (QND). The table given below using the table and graph describes the Inner and Outer Boundary Intrusion Detection with Transductive Learning concepts for effectively detecting the intrusion in the MANET.

NodeCount inOuter Boundary	**Outlier Detection Accuracy (%)**		
	DAD Scheme	QND method	IOBIDS with Transductive Learning concepts
10	75	81	85
20	69	70	75
30	74	76	80
40	83	87	91
50	78	82	86
60	63	65	70
70	74	78	83
80	83	90	95

No. of Connected Nodes	True Positive Value (Precision)		
	DAD Scheme	QND method	IOBIDS with Transductive Learning concepts
4	0.69	0.81	0.89
8	0.71	0.83	0.91
12	0.75	0.84	0.92
16	0.78	0.85	0.93
20	0.79	0.89	0.94
24	0.80	0.90	0.96
28	0.81	0.91	0.97

Table 1 Tabulation for Outlier Detection Accuracy

Table 1 describes the outlier detection accuracy result based on the node count in the outer boundary of mobile ad-hoc network. The node count ranges from 10, 20, 30…80. The outlier detection measurement is used to easily measure the outliers which are intruded in the outer boundary of the mobile network.

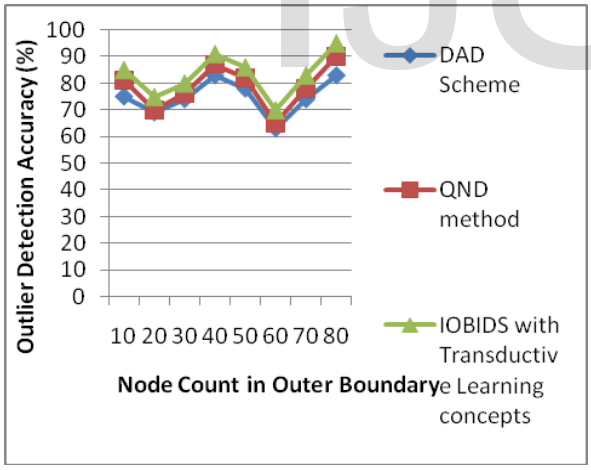


Fig 4 Outlier Detection Accuracy Measure

Fig 4 shows the measure for outlier detection accuracy. Report based outlier detection is the main objective in detecting the outliers in the IOBIDS with Transductive Learning concepts. Report in ROD mechanism refers to the identification of packet dropping which is 8 – 14 % improved when compared to the DAD Scheme [1]. The development of report method in the outlier detection, leads to the improved communication system by removing the intrusion by 4 – 7 % when compared with the QND method [2] on the outer boundary of the MANET.

Table 2 True Positive Value Tabulation

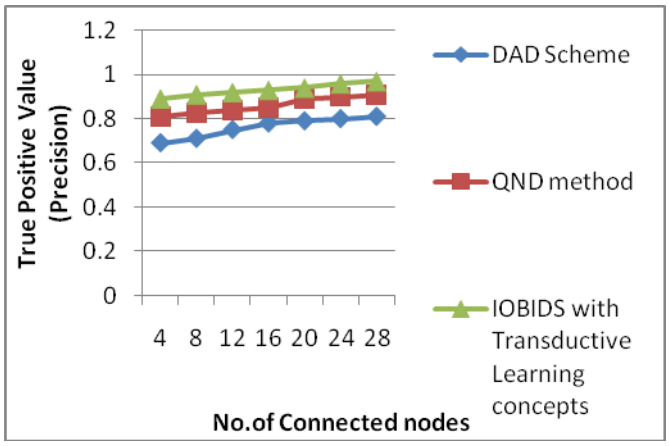


Fig 5 True Positive Value Measure

Fig 5 describes the true positive measure (precision) based on the connected node count in the MANET. Transductive learning merge the Orthomorphic Analyst k-Nearest Neighbor (OANN) method and Report based Outlier Detection (ROD) mechanism for effective detection of intrusion and to compute true positive value. Transductive learning defines the inner and outer structure with the N_i in the MANET leading to the improvement of true positive value from 18 – 28 % when compared with the DAD Scheme [1] and 5– 9 % improved when compared with the QND method [2].

Node count in Inner Boundary	Inner Boundary Analyzing Efficiency (%)		
	DAD Scheme	QND method	IOBIDS with Transductive Learning concepts
10	82	87	90
20	84	90	93
30	86	92	94
40	78	82	86
50	82	87	92

60	79	84	87
70	84	88	93
80	86	90	96

Table 3 Tabulation of Inner Boundary Analyzing Efficiency

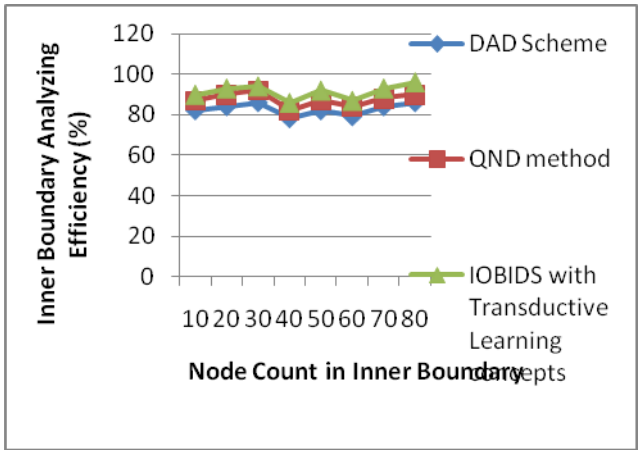


Fig 6 Measure of Inner Boundary Analyzing Efficiency

Fig 6 illustrates the inner boundary analyzing efficiency based on the node count in the inner boundary. With the application of angle based distance measured between the node points for easy detection of the traffic creating nodes in MANET and the inner boundary using the mathematical mapping the correct angles are analyzed for anomalies with the 'i' boundary values. The boundary analyzing efficiency is improved by 9 – 12 % when compared with the DAD Scheme [1] and 2 – 6 % improved when compared with the QND method [2].

Data Packet Size (KB)	Runtime (sec)		
	DAD Scheme	QND method	IOBIDS with Transductive Learning concepts
15	321	245	237
30	355	278	254
45	468	373	324
60	592	512	491
75	422	351	314
90	453	398	371
105	547	478	438
120	667	583	540

Table 4 Tabulation for Runtime Measure

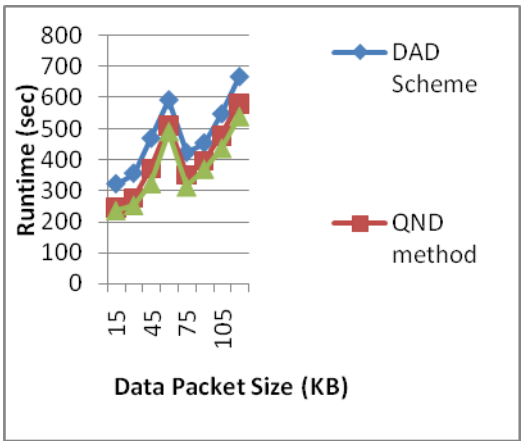


Fig 7 Measure of Runtime

Fig 7 depicts the runtime based on the data packet size. The runtime range varies as the data packet size is increased. The data packet size is measured in terms of Kilo Bytes (KB). The runtime is reduced in IOBIDS with Transductive Learning concepts by using the sorted sequence of the mobile nodes within the boundary points. The boundary nodes between 'i' (i.e.,) source and 'j' (i.e.,) destination in IOBIDS with Transductive Learning concepts reduces the time taken for running the system by 17- 30 % when compared with the DAD Scheme[1] and 3 – 13 % when compared with the QND method [2].

Pause Time (sec)	Packet Loss Rate (%)		
	DAD Scheme	QND method	IOBIDS with Transductive Learning concepts
5	2.55	2.88	1.81
10	3.20	3.82	2.38
15	8.15	9.20	6.12
20	6.68	7.60	5.11
25	4.45	5.65	3.49
30	9.15	10.22	6.37
35	10.3	11.25	7.89

Table 5 Tabulation of Packet Loss Rate

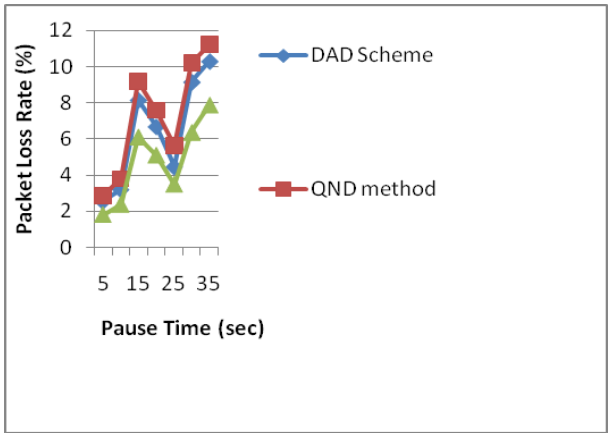


Fig 8 Measure of Packet Loss Rate

Fig 8 demonstrates the packet loss rate based on the pause time. The pause time in the ns2 simulator varies for different size of the packet transmission. The packet loss is measured using Eqn (7) and ROD is used to easily analyze the drop of packets from the MANET. The packet drop percentage is reduced by 21 – 30 % when compared with the DAD Scheme [1] and 29 – 38 % reduced when compared with the QND method [2].

Finally, Inner and Outer Boundary intrusion Detection identifies intrusive activities in MANET and combines the system through transductive learning concept. The inner intrusion detection uses the Orthomorphic Analyst k-Nearest Neighbor (OANN) method with 'i' boundary values for the detection. The outer boundary detection uses the Report based Outlier Detection (ROD) mechanism with 'i' boundary values.

5 Related Work

Intrusion detection system (IDS) plays a very significant role for detecting different types of attacks. The main function of intrusion detection is to protect the network, examine and discover out intrusions among usual assessment data, and measured as a classification problem. Intrusion detection system is into two basic methods namely, misuse detection and anomaly detection methods. Localized Multicast for detecting node replication attacks as described in [15] noticed a node compromising operation with certain probability. Localized Multicast failed to simulate the RED protocol and then had a more thorough comparison of efficiency based on empirical results.

A distributed intrusion detection scheme as illustrated in [8] was based on finite state machine. A cluster dependent detection method was offered and a node was elected as the monitor node for a cluster. These monitor nodes not only make restricted intrusion detection assessment, but also cooperatively take part in global intrusion detection. Design-Based secure leader election model as expressed in [12] elected an optimal collection of leaders to reduce the overall resource expenditure. The resource expenditure acquired an excessive performance overhead.

Quantify Network Dynamism (QND) as described in [2] influenced the mobility from various performance perspectives but failed in effective designing of concrete data diffusion. The undefined procedure was optional and enumerated numerous metrics that affect data availability. QND plan still needed to address the qualitative performance metrics on the mobility models. Redundancy management as illustrated in [5] used the multipath routing to respond user queries in the presence of undependable and malicious nodes. The design vigorously decided the best redundancy stage to relate to multipath routing for intrusion tolerance. The query reaction success probability was maximized while failed to explore the malicious attack on the packet dropping.

6. CONCLUSION

Intrusion detection method on the inner and outer boundary values using transductive learning concept produce the qualitative result. The Orthomorphic Analyst k-Nearest Neighbor and Report based Outlier Detection uses the two different measures to improve its detection ability in mobile ad-hoc network. Orthomorphic Analyst k-Nearest Neighbor used the mathematical mapping of nodes and identifies the traffic intrusion in MANET. The traffic intruded nodes are

identified effectively in the inner boundary range. The Report based Outlier Detection identifies the packet dropping of nodes. Transductive learning concept merges the metrics in MANET. A series of experimental results demonstrate that the inner and outer boundary intrusion detection with the transductive learning concept effectively detect true positive value of transductive concept, and the improved efficiency on 4.437 % inner boundary analyzing. The factors such as runtime for analyzing the outer boundary intrusions and intrusion detection accuracy are clearly examined.

REFERENCES

[1] Hidehisa Nakayama., Satoshi Kurosawa., Abbas Jamalipour., Yoshiaki Nemoto, Senior and Nei Kato., "Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 5, JUNE 2009

[2] Takahiro Hara., "Quantifying Impact of Mobility on Data Availability in Mobile Ad Hoc Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 2, FEBRUARY 2010

[3] Elizabeth M. Daly., and Mads Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANET," IEEE Transactions on Mobile Computing, Vol. 8, No. 5, May 2009

[4] Zhou Sha., Jia-Liang Lu., Xu Li., Min-You Wu., "An Anti-Detection Moving Strategy for Mobile Sink," IEEE Global Telecommunications Conference (GLOBECOM 2010).

[5] Hamid Al-Hamadi and Ing-Ray Chen, "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Network and Service Management, Vol. 10, No. 2, June 2013

[6] R. Nakkeeran., T. Aruldoss Albert., and R.Ezumalai., "Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks," IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010

[7] Haiying Shen., and Lianyu Zhao., "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013

[8] Yi Ping, Jiang Xinghao, Wu Yue & Liu Ning "Distributed intrusion detection for mobile ad hoc network", Journal of Systems Engineering and Electronics Vol. 19, No. 4, 2008

[9] Elhadi, Shakshuki, Nan Kang, Tarek and Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs ", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013

[10] T.Kumanan and Duraiswamy "Dynamic Intrusion Detection with Data Fusion and Aggregation in High-Security Mobile Ad Hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012

[11] Jeyashree, "Highly Secure Distributed Authentication and Intrusion Detection with Data Fusion in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013

[12] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE transactions on dependable and secure computing volume: 8, issue: 1, 2011

[13] R.Nallusamy, K.Jayarajan, Dr.K.Duraiswamy, "Intrusion Detection in Mobile Ad Hoc Networks Using GA Based Feature Selection", Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2009

[14] Ming-Yang Su "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", journal of Elsevier, 2011

[15] Bo Zhu., Sanjeev Setia, Sushil Jajodia., Sankardas Roy., and Lingyu Wang., "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9,

NO. 7, JULY 2010

[16] Tapan P. Gondaliya, Maninder Singh, "Intrusion detection System for Attack Prevention in Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013

[17] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "Intrusion Detection System (IDS) for Combating Attacks against Cognitive Radio Networks Zubair Network", IEEE (Volume: 27, Issue: 3), May-June 2013

[18] Aikaterini Mitrokotsa, Christos Dimitrakakis "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", journal of Elsevier, 2012

[19] Yun Zhou., Xiaoyan Zhu., and Yuguang Fang., "MABS: Multicast Authentication Based on Batch Signature," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010

[20] Marjan Kuchaki Rafsanjani., Ali Movaghar., and Faroukh Koroupi., "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes," World Academy of Science, Engineering and Technology, Vol:20 2008.