ISSN 2319 - 6629
Volume 7, No.5, August - September 2018
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt01752018.pdf
https://doi.org/10.30534/ijwcnt/2018/01752018

An Efficient Intrusion Detection Model Using Adaptive Boosting With Uninterrupted Bayesian Time Mobile Networks

Dr.V. UMADEVI
Principal, New Prince Shri Bhavani Arts and Science College, Chennai, 600100, India
vumadevi76@gmail.com.

ABSTRACT

Mobile Ad-hoc network (MANET) is a wireless system without any infrastructure that consists of mobile nodes such as mobile phones, laptops and Personal Digital Assistants (PDA). The network system with mobile nodes becomes more difficult when an attack is said to occur, resulting in unsecure network path. As a result, a detection system needs to be developed to overcome the intrusion issue. Many secure payment and trust management schemes were introduced with the objective of minimizing the intrusion reducing the computation overhead and improving the reliability. However, an intelligent intrusion detection mechanism is necessary to address the security issues and combat against collusion attack. In this paper, to perform an intelligent intrusion detection model, Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks is developed. Adaptive boosting combines the spanning tree classifier with Uninterrupted Bayesian Timed Mobile nodes in ad hoc network, which in turn increase resource utilization factor. Uninterrupted Bayesian Time Mobile algorithm initializes the weight, depending on the node's class state in the spanning tree and improves the trust accuracy across the ad hoc network. UBTM network works with the active local mobile nodes system using the Stochastic Markov process. The Stochastic Markov process reduces the mobile node sampling along with intrusion detection based on node class weight assigned to corresponding nodes in the ad hoc network. AB-UBTM works together for effectively securing the system when a singular and collusive attack occurs. The analytical and simulation results demonstrate that AB-UBTM network requires much less spanning tree construction time than the existing state-of-the-art works. Moreover, AB-UBTM can secure the network and precisely identify the cheating nodes by improving the trust accuracy. Experimental analysis shows that AB-UBTM network is able to reduce the spanning tree construction time by x% and improves the trust accuracy rate by y% compared to the state-of-the-art works.

Keywords: MANET, Personal Digital Assistants, Adaptive Boosting, Bayesian Time Mobile, Stochastic Markov process

1. INTRODUCTION

Detection of intrusion at an early stage and removal of malicious nodes is one of the most important issue to be addressed in ad hoc network. A secure payment scheme was introduced in [1] using the concept of Accounting Center (AC) with the objective of identifying the cheating nodes and therefore reduce intrusions. Trust management in addition to trust chain optimization was performed in [2] to meet out the path reliability requirements using trust metric. A Denial of service attack to Universal Mobile Telecommunications System was introduced in [3] with the objective of ensuring security.

An intrusion detection model using behavior rule specification was designed in [4] with the objective of providing security. In order to minimize the message delay during jamming by defining jamming process improvement in message transmission rate was ensured. Though security was ensured in all the above said methods, they lack resource utilization which is addressed in our work by designing an Adaptive Boosting algorithm.

One of the hot research issues in the field of ad hoc network is the effective preservation privacy and therefore providing higher intrusion detection model. In [6], a privacy preserving sum and product calculation was introduced with the objective of improving the security. With the objective of reducing the malware attacks in heterogeneous network, encounter-based distribution algorithm was used in [7]. In order to detect the Primary User Emulation (PUE) [8] attack correlation between RF signals were measured to reduce the false positive rate in a significant manner.

Damage caused by Vampire attacks was analyzed in [9] with the aid of network wide energy usage factor to mitigate attack at an early stage. Secure data aggregation

was performed in [10] to provide mechanism against collusion attacks. Though security was ensured in the above said methods by mitigating attack at an early stage, the accuracy with which security was provided remained unaddressed.

Measuring abnormalities and fixing the issues in ad hoc network is one of the major concerns to many academicians. In [11], Spearman's rank correlation coefficient was used for handling data in a segment based manner resulting in minimizing the communication cost. Ensuring measures against flood attacks was introduced in [12] with the aid of claim-carry-and-check scheme. Cooperative caching mechanisms was introduced in [13] with the objective of improving the data access performance in a significant manner. Cross-layer approach was designed in [14] using probabilistic correlated failure model to ensure normalcy in traffic by reducing the interference node.

A novel task and resource allocation control framework was introduced in [15] using interference-aware scheduler to increase the throughput on virtualized servers. In [16], mechanisms to address issues related to multiple spoofing were introduced with the objective of improving the rate of accuracy in a significant manner. In [17], a dynamic anomaly detection scheme was designed to identify the malicious hosts at an early stage using projection distances. A secure leader election model [18] was designed for efficient intrusion detection in MANET. Bayesian filters were applied in [19] to combat against black hole attacks.

Based on the above said methods, the proposed work Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks takes into account the dynamically changing conditions in MANET environments. Our aim is to design and evaluate an efficient intrusion detection model and improve the trust accuracy by improving the security and therefore minimizing the intrusion rate.

The contributions of this work are as follows. First, Adaptive Boosting is designed with the objective of improving the resource utilization factor through probability distribution. Second, Uninterrupted Bayesian Time Mobile (UBTM) algorithm is introduced with the objective of improving the trust accuracy rate. Finally, security and rate of intrusion being detected is improved by applying stochastic markov process with the aid of function intensity.

The rest of this paper is organized as follows. Section 2 discusses intrusion detection model and describes our proposed Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks. Section 3 develops the AB-UBTM Networks performance model and describes how the AB-UBTM networks can be used to evaluate system behaviors under the proposed intrusion detection model. Section 4 gives numerical results obtained through the evaluation of our performance AB-UBTM networks with the aid of table values and graph form. Finally, Section 5 concludes our paper.

2. DESIGN OF ADAPTIVE BOOSTING WITH UNINTERRUPTED BAYESIAN TIME MOBILE (AB-UBTM) NETWORKS

In this section, an overview description of intelligent intrusion detection mechanism is designed and then, the Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks is presented. One of the most important roles played by MANET is security that provides effective network service without any malicious attack. Intrusion detection monitors the activities in a mobile system by collecting information and then analyzing them. Figure 1 shows the architecture diagram of Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks.

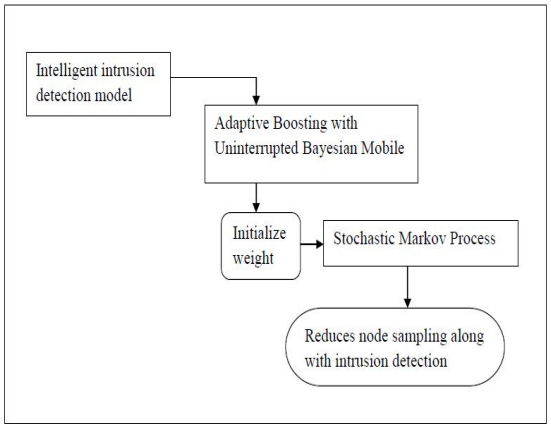

Figure 1 Architecture diagram of AB-UBTM Networks

Figure 1 given above shows the architecture diagram of AB-UBTM Networks. With the objective of designing a full proof intelligent intrusion detection model, adaptive boosting with uninterrupted Bayesian mobile is designed. With the initialization of weight depending on the mobile nodes class state, resource utilization factor is improved. Next, by designing Uninterrupted Bayesian Time

Mobile algorithm, the trust accuracy is improved based on the conditional probability in addition to priori and posterior probability of mobile nodes. Therefore trust accuracy is improved reducing the intrusion. Finally with the design of stochastic markov process, intrusion is reduced at an early stage using functional intensity.

2.1 Construction of Adaptive Boosting

Adaptive boosting combines the spanning tree classifier with Uninterrupted Bayesian Timed Mobile nodes in ad hoc network. With the classified intrusions from spanning tree classifier, Uninterrupted Bayesian Timed Mobile nodes in ad hoc network are applied with the objective of improving the resource utilization.

Adaptive boosting in AB-UBTM initially assigns a weight and adaptively updates the weights during each round of boosting using Uninterrupted Bayesian Timed Mobile nodes. The traces of log files in network that are misclassified have increased weight, whereas those that are classified correctly have their weight decreased. Figure shows the block diagram of Uninterrupted Bayesian Timed Mobile node.

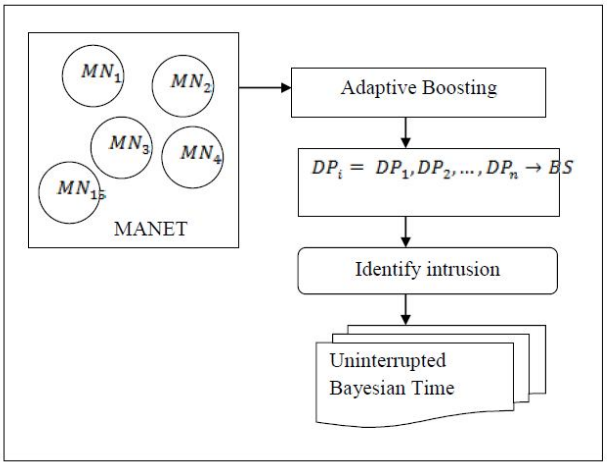

Figure 2 Block diagram of Uninterrupted Bayesian Timed Mobile nodes

As shown in the figure 2, let us consider the mobile nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$' in MANET network '$MN$' setting at time interval 't' sending data packets '$DP_i = DP_1, DP_2, \ldots, DP_n$' to base station '$BS$'. Then, a malicious node refrains from delivering a data packet '$DP_i = DP_1, DP_2, \ldots, DP_n$' with probability '$\alpha_i$'. Let '$Prob$' denotes the probability, then a probability distribution is said to occur as given below

$$Prob_i^j = prob_i^j \quad (1)$$

$$Prob_i^j = 1 - prob_i^j \quad (2)$$

From (1) and (3), the mobile node's 'i' view probabilities about mobile node 'i' over the base station 'BS' is provided with the probability of success and failure factor. Followed by the probability factor, each mobile node payoff is evaluated which is the residue between the mean utility and the mean cost given the views of node 'i' about the types of all mobile nodes in the ad hoc network. The vector representation of all mobile nodes is as given below

$$MN_p^q = [\ldots MN_1^2 \ldots MN_i^j], where\ p, i \in MN \quad (3)$$

From (3), the vector 'MN_p^q' represents the view of mobile node 'i' about the mobile node 'j' which is in the ad hoc network 'MN' respectively. Figure 3 shows the algorithmic description of Adaptive Boosting.

Input : Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', Time interval '$t$', Data Packet '$DP_i = DP_1, DP_2, \ldots, DP_n$', Base Station '$BS$'
Output: optimized resource utilization
Step 1: **Begin** Step 2: **For** each Mobile Nodes 'MN_i' Step 3: Identify the probability distribution factor using () and () Step 4: Measure payoff using () Step 5: **End for** Step 7: **End**

Figure 3 Adaptive Boosting algorithm

From the above algorithm (Figure 3), the probability distribution factor and payoff is measured for each mobile node at different time intervals. The evaluation of probability of success and failure factor increases the resource utilization factor substantially. With the with Uninterrupted Bayesian Timed Mobile nodes, the class

conditional probability is efficiently estimated using the vector representation of mobile nodes, given the class label 'CL'.The formulation of Uninterrupted Bayesian Timed Mobile nodes is formulated as given below

$$P\left(MN_p^q, CL\right) = \sum_{i=1}^{n} \left(\frac{MNi_p^q}{CL}\right) \qquad (4)$$

where mobile nodes 'MN_i' consists of 'i' mobile node. The AB-UBTM networks instead of evaluating the class label probability for every combination of mobile nodes 'MNi', the proposed work with the objective of improving the resource utilization factor, only estimate the conditional probability of each MNi', given class label 'CL'.

2.2 Uninterrupted Bayesian Time Mobile algorithm

Once, the conditional probability of mobile nodes is provided with class labels with the objective of improving the resource utilization, the AB-UBTM networks construct an Uninterrupted Bayesian Time Mobile (UBTM) algorithm. The UBTM algorithm initializes the weight, depending on the node's class state in the spanning tree and improves the trust accuracy across the ad hoc network. Figure 4 shows the block diagram of Uninterrupted Bayesian Time Mobile.

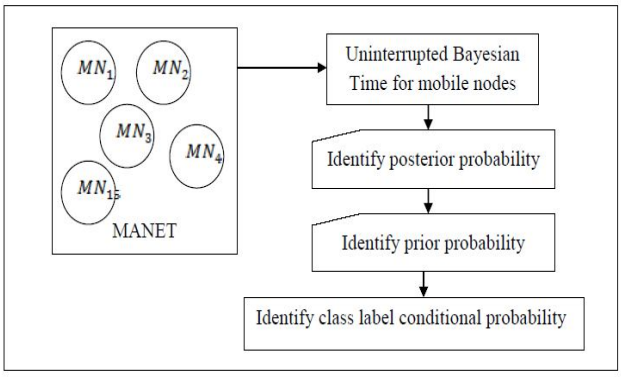

Figure 4 Block diagram of Uninterrupted Bayesian Time Mobile

As shown in the figure 4, in order to classify a test sample, the UBTM algorithm evaluates the posterior probability for each class label 'CL' and is formulated as given below

$$Posterior\left(\frac{CL}{MN_i}\right) = \left(\frac{Prob(CL)\sum_{i=1}^{n} Prob\left(\frac{MN_i}{CL}\right)}{Prob\ (MN)}\right) \qquad (5)$$

From (5), the posterior probability for each class label is evaluated in an efficient manner. This in turn improves the trust accuracy and combat against the collusion attacks. Furthermore using AB-UBTM networks, the prior probability for each class label is evaluated by measuring how often each mobile node flows through a specific network. For each mobile nodes 'MN_i', the number of occurrences of each mobile node in AB-UBTM networks is identified to determine the prior probability for each class label. This prior probability helps in improving the trust accuracy.

The class label conditional probability for AB-UBTM networks is also measured as given below

$$Prior\left(\frac{MNi_p^q}{CL_i}\right) = Total\ occurrence\ (MN_i|MN) \qquad (6)$$

From (6), the class conditional probabilities for each mobile nodes 'MNi_p^q' is measured by counting the total number of occurrences of the mobile nodes 'MN_i' in the ad hoc network 'MN'. Then the UBTM algorithm classifies all the training examples with these prior and posterior values (using x and y respectively) in ad hoc network that efficiently classifies depending on the class node's stage improving the trust accuracy.

Let us consider a network 'MN' that has independent mobile node 'MN_e', the AB-UBTM networks already knows the '$Prob(\frac{MN_i}{CL_i})$', for each class label 'CL_i' and mobile node 'MN_i'. Then, the AB-UBTM networks evaluates '$Prob\left(\frac{MN_e}{CL_i}\right)$' and is mathematically formulated as given below

$$Prob\left(\frac{MN_e}{CL_i}\right) = Prob\ (CL_i)\sum_{i=1}^{n} \frac{MN_i}{CL_i} \qquad (7)$$

From (7), the probability that 'MN_e' is in a class label is identified based on the conditional probability and prior probability for that class label. Followed by this, the

AB-UBTM networks identify the posterior probability for each class label and therefore the classification is made in an efficient manner improving the trust accuracy of the ad hoc network. Figure 5 shows the algorithmic description of UBTM

Input: Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', Class Label '$CL$',
Output: Efficient classification of the network reducing the intrusion
Step 1: **Begin** Step 2: **For** each Mobile Nodes 'MN_i' Step 3: Evaluate the posterior probability using () Step 4: Evaluate prior probability using () Step 5: Measure conditional probability using() Step 6: **End for** Step 7: **End**

Figure 5 UBTM algorithm

The figure 5 given above shows the algorithmic description of UBTM. The UBTM algorithm in the proposed work performs efficient classification of the network and therefore reducing the intrusion rate. With the objective of improving the trust accuracy, the posterior probability, prior probability and conditional probability for each mobile nodes is evaluated. This therefore ensures efficient classification of the ad hoc network and therefore improves the trust accuracy of the network.

2.3 Stochastic Markov process

Finally, the UBTM network works with active local mobile nodes system using the Stochastic Markov process based on node class weight assigned to corresponding nodes in the ad hoc network. With the application of Stochastic Markov process, the mobile node sampling along with intrusion detection is reduced in a significant manner. As a result, the AB-UBTM works together for effectively securing the system when a singular and collusive attack occurs.

The Stochastic Markov process in AB-UBTM network proceeds with an inceptive dissemination '$Diss_i^0$' in a given ad hoc network '$MN(t)$ = '$MN_1, MN_2, \ldots, MN_n$' and is formulated using intensities as given below

$$I_i = \begin{bmatrix} -i_{MN_1} & i_{MN_1 MN_2} & -i_{MN_1 MN_n} \\ i_{MN_2 MN_1} & -i_{MN_2} & i_{MN_2 MN_1} \\ i_{MN_n MN_1} & i_{MN_1} & -i_{MN_n} \end{bmatrix} \quad (8)$$

From (8), '$i_{MN_i MN_j}$' refers to the transition (i.e. mobility) from state 'MN_i' to 'MN_j' respectively. Therefore, the behavior of '$MN(t)$' is described as follows. The mobile node 'MN_i' stays in the prescribed position 't' according to the exponential distribution as formulated in (8).Therefore, the functional intensity with which the mobile nodes in AB-UBTM network remains at 't' is formulated as given below.

$$f(I_i, t) = \exp(I_i, t) \quad (9)$$

From above formulation (i.e. functional intensity), the Stochastic Markov process minimizes the mobile node sampling along with intrusion detection based on node class weight assigned to corresponding nodes in the ad hoc network. The intrusion detection based on node class weight assigned to corresponding nodes is formulated as given below

$$MN_i W_i = \left(\frac{Prob(f(I_i, t))}{f(I_i)} \right) \quad (10)$$

From (10), the nodes class weight '$MN_i W_i$' is used as the basis for effectively securing the entire ad hoc network. This improves the security and rate of intrusion being detected at an early stage.

3. EXPERIMENTAL SETTINGS

Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks in mobile ad hoc network uses the NS-2 simulator with the network range of 1500 * 1500 m size. Mobile nodes selected for experimental purpose is 70 nodes. Experiments are conducted using Destination Sequence Based Distance Vector DSDV as routing protocol for AB-UBTM networks.

The AB-UBTM networks moving speed of the mobile nodes in MANET is about 15 m/s for each mobile node with a simulation rate of 45 seconds to perform data packet transmission between mobile nodes. The parametric values for performing experiments are shown in table 1.

Experiment is conducted on the factors such as resource utilization factor, trust accuracy, security, rate of intrusion being detected with respect to node density and packets being transmitted in MANET. The results of the metrics of AB-UBTM networks is compared against the existing methods such as Secure Payment with Low Communication and Processing Overhead (SP-LCPO) [1] and Trust Management using Trust Chain Optimization (TM-TCO) [2] respectively.

Table 1 Parametric settings

Parameters	Values
Simulator	NS 2.34
Simulation area	1500 m * 1500 m
Simulation time	45 sec
Mobile node density	10, 20, 30, 40, 50, 60, 70
Data packet	512 bytes/packet
Data packet transmission range	30 m, 60 m, 90 m
Movement model	Random waypoint

Resource utilization measures the ratio of available nodes to the nodes being utilized. The mathematical formulation of resource utilization is as given below

$$RU = \left(\frac{Nodes_{util}}{Nodes_{avail}}\right) * 100 \quad (11)$$

From (11), the resource utilization 'RU' is measured using available nodes '$Nodes_{avail}$' and utilized nodes '$Nodes_{util}$'. Higher the resource utilization, more efficient the method is said to be. Trust accuracy is measured using the class label that efficiently classifies depending on the class node's stage with respect to node density. It is measured in terms of percentage (%).

$$TA = \sum_{i=1}^{n} \left(\frac{CL_i}{Node\ density}\right) * 100 \quad (12)$$

From (12), the trust accuracy '' is measured with the help of class label '' and total number of nodes in the network considered for experimental evaluation. Higher the trust accuracy, more efficient the method is said to be. Security is obtained based on the difference between the packets being transmitted and the packets dropped during transmission. The mathematical formulation for security is as given below.

$$S = (Packets_s - Packets_d) \quad (13)$$

From (13), security 'S' is measured using packets transmitted '$Packets_s$' and packets dropped '$Packets_d$' respectively. Security is measured using packets per second (PPS). Higher the security, more efficient the method is said to be.

4. DISCUSSION

Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks is compared against the existing Secure Payment with Low Communication and Processing Overhead (SP-LCPO) [1] and Trust Management using Trust Chain Optimization (TM-TCO) [2]. Table 2 evaluates the resource utilization factor in terms of percentage achieved with different number of nodes ranging from 10 to 70 and comparison is made with the two existing methods namely, SP-LCPO [1] and TM-TCO [2].

Table 2 Tabulation for resource utilization

Node density	Resource utilization (%)		
	AB-UBTM	SP-LCPO	TM-TCO
10	71.35	61.45	51.85
20	75.83	63.78	58.74
30	80.326	68.27	63.23
40	74.19	62.14	57.10
50	79.35	67.30	62.26
60	78.45	66.40	61.36
70	84.35	72.30	67.26

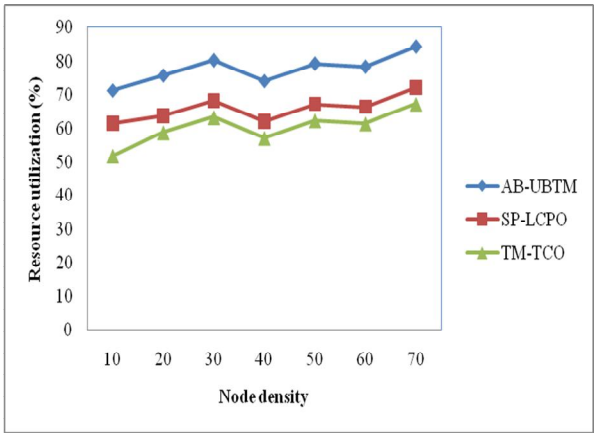

Figure 6 Measure of resource utilization

Figure 6 shows the resource utilization based on the number of nodes in the range of 10 and 70. The resource utilization for differing node density is measured based on the available and utilized nodes in ad hoc network. From the figure it is evident that the resource utilization using the proposed method is comparatively greater than the two other existing methods. This is because by applying the Adaptive Boosting adaptively updates the weights during each round of boosting using Uninterrupted Bayesian Timed Mobile nodes. This in turn improves the resource utilization in AB-UBTM networks by 15.05% compared to SP-LCPO. In addition, each mobile node payoff is evaluated which are the residue between the mean utility and the mean cost given the views of node further increases the resource utilization rate by 23.79% compared to TM-TCO respectively.

Table 3 Tabulation for trust accuracy

Node density	Trust accuracy (%)		
	AB-UBTM	SP-LCPO	TM-TCO
10	71.29	61.35	52.45
20	75.99	70.94	66.89
30	82.35	77.30	73.25
40	80.48	75.43	71.38
50	84.55	79.50	74.45
60	82.19	75.14	71.09
70	87.32	82.27	78.22

Table 2 represents the comparison results of trust accuracy level and performance with node density in the range of 10 to 70 mobile nodes in ad hoc network considered for experimental purpose.

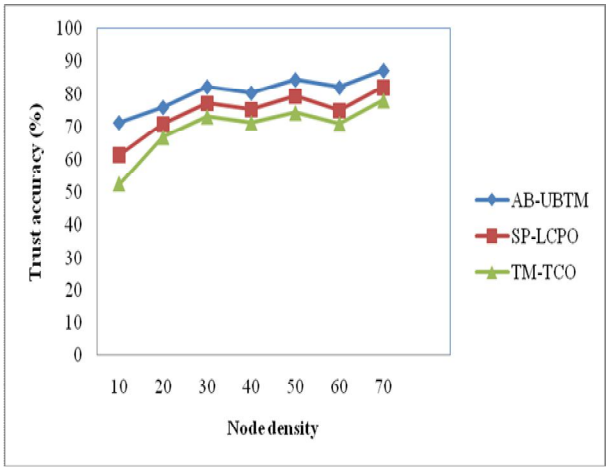

Figure 7 Measure of trust accuracy

Figure 7 shows the trust accuracy efficacy level of AB-UBTM networks, SP-LCPO and TM-TCO for 10 to 70 nodes in ad hoc network. The performance of all trust accuracy efficacy level is improved as the number of nodes increases though minimizes for 40 mobile nodes considered. But comparatively, the trust accuracy level is increased in the proposed AB-UBTM networks when compared to two other methods. For example, for node density of MN = 20, the percentage trust accuracy efficacy level improvements of AB-UBTM networks over SP-LCPO [1] and TM-TCO [2] are on the order of 6.64 percent and 11.97 percent respectively. This is because by applying Uninterrupted Bayesian Time Mobile (UBTM) algorithm that initializes the weight, depending on the node's class state and therefore increases the trust accuracy level by 9.86% compared to SP-LCPO. In addition, by evaluating the posterior and prior probability for obtaining conditional probability efficiently classifies depending on the class node's stage improving the trust accuracy by 18.42 % compared to TM-TCO respectively.

Table 4 Tabulation for security

Packets being sent (KB)	Security (PPS)		
	AB-UBTM	SP-LCPO	TM-TCO
50	45	42	39
100	82	67	62
150	135	120	115
200	175	160	155
250	210	195	190
300	240	225	220
350	280	260	255

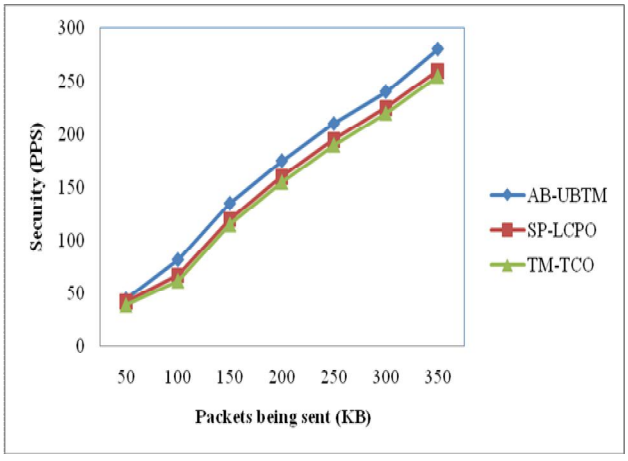

Figure 8 Measure of security

Table 3 and figure 8 shows the security using the proposed AB-UBTM networks and comparison is made with two other methods with different number of packets being sent in terms of kilobytes (KB). The experimental results show that the AB-UBTM networks efficiently secure the system on different packets being sent is higher than that of SP-LCPO [1] and TM-TCO [2] respectively. This is because of the fact that by applying the Stochastic Markov process, the mobile node sampling is reduced based on node class weight assigned to corresponding nodes in the ad hoc network resulting in increasing the security by 12.27% compared to SP-LCPO. Furthermore, by applying functional intensity, class weight is used as the basis for effectively securing the entire ad hoc network resulting in increasing the security using AB-UBTM networks by 16.36% compared to TM-TCO respectively.

Table 5 Tabulation for rate of intrusion being detected

Method	Rate of intrusion being detected
AB-UBTM	81.38
SP-LCPO	75.42
TM-TCO	61.15

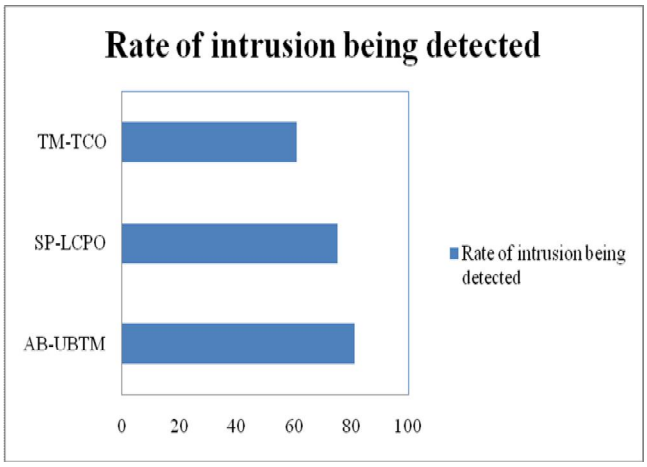

Figure 9 Measure of intrusion rate being detected

Table 5 and figure 9 measures the rate of intrusion being detected with respect to different node density in the range of 10 to 70 mobile nodes with packets in the range of 50 KB to 350 KB. As shown in the figure, the intrusion rate being detected efficiently at an early stage is improved using AB-UBTM when compared to the two other methods SP-LCPO and TM-TCO respectively. This is because by applying Adaptive Boosting and UBTM algorithm in an extensive manner, efficient intrusion detection model is designed and combat against collusion attacks. As a result, the intrusion rate being detected is improved by 7.32% compared to SP-LCPO and improved by 18.92% compared to TM-TCO respectively.

5. CONCLUSION

An Adaptive Boosting with Uninterrupted Bayesian Time Mobile (AB-UBTM) Networks for improving the trust accuracy rate of intrusion detection model is presented. This mechanism has been designed to enhance the security level for different mobile nodes in ad hoc network using the Uninterrupted Bayesian Time Mobile algorithm. We adopt Adaptive Boosting algorithm to improve the resource utilization factor using probability of success and failure factor. Next, an Uninterrupted Bayesian Time Mobile (UBTM) is designed depending on the node class state to increase the trust accuracy rate. The proposed AB-UBTM networks uses the posterior and prior probability for each class label by measuring how often each mobile node flows through a specific network to determine the rate of intrusion. In addition, the class conditional probability for each mobile node is measured by counting the total number of occurrences of the mobile nodes in ad hoc network at less time and therefore improves the intrusion detected rate being detected at an early time. Experimental evaluation is conducted to improve the evaluation and measured the performance in terms of resource utilization factor, trust accuracy rate, rate of intrusion being detected and security with respect to node density and different packets of different sizes. Performance results reveal that the proposed AB-UBTM networks provides higher resource utilization rate and therefore improves the trust accuracy rate and strengthen the overall mechanism. Compared to the existing methods SP-LCPO and TM-TCO, the proposed AB-UBTM networks improve the resource utilization factor by 19.42% and trust accuracy rate by 14.14%.

ACKNOWLEDGEMENT

I have taken efforts in this work. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I would like to express my gratitude towards my parents & family members for their kind co-operation and encouragement which help me in completion of this paper.

My thanks and appreciations also go to my colleague in developing the paper and people who have willingly helped me out with their abilities.

REFERENCES

1. Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, **"A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks",** *I*EEE Transactions on Parallel and Distributed Systems *(TPDS), Volume 24, Issue 2, February 2013, Pages 209 – 224.*
2. Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, **"Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks",** *Elsevier, Volume 35, Issue 3, May 2012, Pages 1001–1012.*
3. Alessio Merlo, Mauro Migliardi, Nicola Gobbo, Francesco Palmieri and Aniello Castiglione, **"A Denial of Service Attack to UMTS Networks Using SIM-Less Devices",** *IEEE Transactions on Dependable and Secure Computing, Volume 11, Issue 3, May-June 2014, Pages 280 – 291.*
4. Robert Mitchell and Ing-Ray Chen, **"Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems"**, *IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January – February 1 2015, Pages 16 – 30.*
5. Zhuo Lu, Wenye Wang and Cliff Wang, **"Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming",** *IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January – February 1 2015, Pages 31 – 44.*
6. Taeho Jung, Xiang-Yang Li and Meng Wan, **"Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel"**, *IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January – February 1 2015, Pages 45 – 57.*
7. Yong Li, Pan Hui, Depeng Jin, Li Su and Lieguang Zeng, **"Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices",** *IEEE Transactions on Mobile Computing, Volume 13, Issue 2, February 2014, Pages 377 – 391.* https://doi.org/10.1109/TMC.2012.255
8. Shaxun Chen, Kai Zeng and Prasant Mohapatra, **"Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space"**, *IEEE Transactions on Mobile Computing, Volume 12, Issue 3, March 2013, Pages 401 – 411.* https://doi.org/10.1109/TMC.2011.272
9. Eugene Y. Vasserman and Nicholas Hopper, **"Vampire attacks: Draining life from wireless ad-hoc sensor networks"**, *IEEE Transactions on Mobile Computing, Volume 12, Issue 2, February 2013, Pages 318 – 332.* https://doi.org/10.1109/TMC.2011.274
10. Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino and Sanjay Jha, **"Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks"**, *IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January – February 1 2015, Pages 98 – 110.*
11. Miao Xie, Jiankun Hu and Song Guo**, "Segment-Based Anomaly Detection with Approximated Sample Covariance Matrix in Wireless Sensor Networks",** *I*EEE Transactions on Parallel and Distributed Systems *(TPDS), Volume 26, Issue 2, February 2015, Pages 574 – 583.* https://doi.org/10.1109/TPDS.2014.2308198
12. Qinghua Li, Wei Gao, Sencun Zhu and Guohong Cao, **"To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks"**, *IEEE Transactions on Dependable and Secure Computing, Volume 10, Issue 3, May - June 2013, Pages 168 – 182.* https://doi.org/10.1109/TDSC.2012.84
13. Wei Gao, Guohong Cao, Arun Iyengar and Mudhakar Srivatsa, **"Cooperative Caching for Efficient Data Access in Disruption Tolerant Networks",** *IEEE Transactions on Mobile Computing, Volume 13, Issue 3, March 2014, Pages 611 – 625.* https://doi.org/10.1109/TMC.2013.33
14. Qiang Zheng, Guohong Cao, Thomas F. La Porta and Ananthram Swami**, "Cross-Layer Approach for Minimizing Routing Disruption in IP Networks",** *I*EEE Transactions on Parallel and Distributed Systems *(TPDS), Volume 25, Issue 7, July 2014, Pages 1659 – 1669.* https://doi.org/10.1109/TPDS.2013.157
15. Ron C. Chiang and H. Howie Huang, **"TRACON: Interference-Aware Scheduling for Data-Intensive Applications in Virtualized Environments",** *I*EEE Transactions on Parallel and Distributed Systems *(TPDS), Volume 25, Issue 5, May 2014, Pages 1349 – 1358.* https://doi.org/10.1109/TPDS.2013.82
16. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe and Jerry Cheng, **"Detection and Localization of Multiple Spoofing Attackers in Wireless Networks",** *I*EEE

Transactions on Parallel and Distributed Systems *(TPDS), Volume 24, Issue 1, January 2013, Pages 44 – 58.*
https://doi.org/10.1109/TPDS.2012.104

17. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto and Nei Kato, **"A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks",** *IEEE Transactions on Vehicular Technology*, Volume 58, Issue 5, June 2009, Pages 2471 – 2481.
https://doi.org/10.1109/TVT.2008.2010049
18. 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, January - February 2011, Pages 89 – 102.*
https://doi.org/10.1109/TDSC.2009.22
19. Jorge Hortelano, Carlos T. Calafate, Juan Carlos Cano, Massimiliano de Leoni, Pietro Manzoni and Massimo Mecella, **"Black-Hole Attacks in P2P Mobile Networks Discovered through Bayesian Filters"**, *Springer, Volume 6428, 2010, Pages 543 – 552.*
20. Attada Venkataramana , S. Pallam setty, " **Analyzing the impact of Simulation Area on the Performance of AODV, DSR, AOMDV and DSDV Routing Protocols for MANETS under Two-ray and Shadowing Propagation Models " ,** *International Journal of Wireless Communications and Networking Technologies, Volume 3, No.1, December – January 2014.*